The International Legal Limitations On Information Warfare

By
Gregory John O'Brien

B.A. September 1982, Saint Joseph's University
J.D. May 1986, Temple University Law School

A Thesis submitted to

The Faculty of

The George Washington University
Law School
in partial satisfaction of the requirements
for the degree of Master of Laws

May 24, 1998

Thesis directed by
Ralph Gustav Steinhardt
Professor of Law

Table of Contents

THE INTERNATIONAL LEGAL LIMITATIONS ON INFORMATION WARFARE

We live in an age that is driven by information. Technological breakthroughs . . . are changing the face of war and how we prepare for war.[1]

Information war has no front line. Potential battlefields are anywhere networked systems allow access – oil and gas pipelines, for example, electric power grids, telephone switching networks. In sum, the U.S. homeland may no longer provide a sanctuary from outside attack.[2]

A panel of Defense Department experts recently warned the nation about the prospect of an electronic Pearl Harbor, a crippling sneak attack on the nation's defense and civilian information systems in which "cyberterrorists" and other unknown assailants cripple the nation's, or the world's, computer-networked communications, financial, and national defense systems.[3]

As the nations of the world become more firmly entrenched in what many have described as the "third wave,"[4] or the "information revolution," the improvements to all levels of society are palpable. The increases in network connections throughout the world have improved communications, made commercial trade more efficient, and provided access to information previously thought unimaginable. Unfortunately, as with the previous world-changing "revolutions," this third wave has also created a change in the way power is allocated among and security is threatened by nations. In a paradoxical way, the information revolution

---

[1] Dr. William Perry, former Secretary of Defense, quoted in Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR 1 (RAND Corporation Report 1996) (*hereinafter* RAND report).

[2] *Id.*

[3] *The Threat of Computer Warfare*, Chicago Tribune, Feb. 8, 1997, at A18.

[4] Richard W. Aldrich, *The International Legal Implications of Information Warfare*, OCCASIONAL PAPER NO. 9, at 6 (Institute for National Security Studies, U.S. Air Force Academy April 1996).

promises the greatest contributions to mankind's development since the agrarian or industrial revolutions but also has the potential to wreak great havoc and turmoil on the world.

All over the world, states are examining the ways this information revolution can be used to ensure national and world security. At the same time, these states are determining the ways in which this revolution can threaten security. With the rise in the world's dependence on the "information highway" has come a commensurate rise in the number of information bandits along that highway who have the ability to crack "cybersafes" and steal money; infiltrate national defense information systems; and issue extortionate threats to key elements of a nation's infrastructure like air traffic control systems or communications networks or electrical power control systems.

The study of the impact of the information revolution on traditional concepts of warfare has only begun over the last few years. Just as the information revolution has dramatically changed life in general, it has similarly created a "revolution in military affairs" in the world's militaries.[5] Concepts and techniques of what has quickly become known as "information warfare" are being studied and developed the world over. This revolution promises to change the way future wars are waged.

The growth of information warfare has also spawned a revolution of sorts in the legal aspects of waging war. Traditional notions of warfare and the customary laws resulting from them are being challenged in a way never anticipated when those laws began their development. Because of the nature of this new medium and the

---

[5] Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 Harv. Int'l L. J. 272, 273 (1996).

way it can be used as a method of warfare, it is unclear how amenable traditional concepts of the laws of armed conflict will be to information warfare.

This paper will examine the ways these traditional concepts are challenged and will attempt to suggest proposals for those areas in which traditional concepts might not be susceptible to a clean application to developing notions of information warfare. Part I of this paper will set forth background information about information warfare – how it is defined; how it is currently employed; how it is developing into a threat to world security. Part II will be a discussion of the laws governing the use of force in the post-Charter age, including the traditional laws of armed conflict, and an examination of how these laws apply or do not apply to this developing method of warfare. It is noted at the outset that this discussion will not include an examination of "conventional" methods of information warfare, like targeting sites with bombs, missiles, or other munitions. Those methods are sufficiently limited presently by the existing laws governing the use of force. Part III will conclude with recommendations for a possible course of action to accommodate this developing method of warfare.

I. Information Warfare Background

A. The Global Information Infrastructure

The global information infrastructure (GII) is a combination of facilities, services, and people which allows anyone from any place to send and receive information when and where they want to at an affordable cost on a nearly

instantaneous basis.[6] It includes the physical facilities used to transmit, store, process, and display voice, data, and images.[7] As a reflection of the progress information technology has made in a relatively short period of time, the first transatlantic cable message in 1858, consisting of 90 words, took over 16 hours to transmit.[8] Fifteen years ago, few cellular telephones or computers existed, and Internet access was limited.[9] Today, there are about 180 million computers in the United States, and, worldwide, there are about 1.3 million local area networks.[10]

The backbone of this infrastructure in many ways is the Internet. The Internet is not really a thing. Rather, it is a collection of many things.[11] The Internet is better conceived as the potential connection of any of millions of computers around the world.[12] Each computer on the Internet is managed independently by persons using common communications standards; a packet switching network, for example, sorts data into standard packets then routes these packets to destinations via an indeterminate number of intermediate routing stations.[13]

---

[6] Peter N. Weiss & Peter Backlund, BORDERS IN CYBERSPACE 302 (Brian Kahin & Charles Nesson ed. 1997).

[7] *Id.*

[8] Sandra K. Kinkaid, *The Record Carrier Industry*, in Am. Bar Ass'n, TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 78 (Anne W. Branscomb ed. 1986)(*hereinafter* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS).

[9] CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES (*hereinafter* CRITICAL FOUNDATIONS), The Report of the President's Commission on Critical Infrastructure Protection, 9 (October 1997).

[10] *Id.*

[11] A. Michael Froomkin, *The Internet As A Source of Regulatory Arbitrage*, 130, in BORDERS IN CYBERSPACE, *supra* note 6.

[12] *Id.*

[13] Froomkin, *supra* note 11, at 130; Kanuck, *supra* note 5, at 272.

The creator of the Internet, the U.S. Department of Defense (DOD), was attracted in the late 1960's to this seemingly anarchical way of sending and receiving information since DOD wanted a communications system that could still function even after a major catastrophe, like a nuclear attack, destroyed a large fraction of the system.[14] Thus, the Internet allows messages to reach their destinations through one of many different routes between computers.[15]

Throughout the world, nations have invested heavily in linking their states with other parts of their countries and with the rest of the world. In the U.S., over $2 billion has been spent on research to find a way to electronically connect nationwide schools, libraries, hospitals, and clinics by the year 2000.[16] In the European Union, over $3.8 billion has been spent to support the new information infrastructure in the EU, while in Japan, the government is spending between $150 and 230 billion to connect every school, home, and office by the year 2015.[17] A recent G-7 ministers' conference on the information society concluded that a smooth and effective transition to an information society is one of the most important tasks to be undertaken in the last decade of this century.[18]

---

[14] Froomkin, *supra* note 11 at 131; Sean Selin, Comment, *Governing Cyberspace: The Need for an International Solution*, 32 Gonz. L. Rev. 365, 367-368 (1997).

[15] Selin, *supra* note 14, at 367.

[16] Henrikas Yushkiavitshus, *Law, Civil Society and National Security: International Dimensions*, in THE INFORMATION REVOLUTION AND NATIONAL SECURITY 46-47 (Stuart J.D. Schwartzstein ed., Center for Strategic and International Studies 1996).

[17] *Id.*

[18] *Id.*

This information technology explosion has dramatically changed most aspects of private, commercial, and public lives and business. Profound change in the marketplace, interdependency, restructuring, and reliance on technology have resulted in the global economy's irreversible commitment to the GII.[19] The GII and its component national information infrastructures (NII) have developed into complex management systems with substantial information-based resources involving the control of electric power, the flow of money, air traffic control systems, and oil and gas production and use.[20]

B. Threats to the GII

Cyberspace has no territorially-based boundaries because the cost and speed of message transmission on the Internet is almost entirely independent of physical location: messages can be transmitted from any physical location to any other site without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another.[21] To complicate matters, the domains used in the process of transmitting information do not necessarily indicate their place of origin. For example, one might have a domain name associated with a server in a different physical location; a server with ".UK" as a domain name might not be in the United Kingdom, and ".com" could indicate

---

[19] CRITICAL FOUNDATIONS *supra* note 9, at 10.

[20] RAND Report *supra* note 1, at xiii.

[21] David R. Johnson & David G. Post, *The Rise of Law on the Global Network*, in BORDERS IN CYBERSPACE *supra* note 6, at 8-9.

physical presence anywhere in the world.[22] Thus, users are generally unaware of the physical location of the pieces of hardware in a network, and, consequently, it is extremely difficult to trace the place of origin of a particular piece of computer information.

This interconnection and anonymous placelessness of the GII have created a set of vulnerabilities the study of which has only recently begun.[23] Today, a computer can cause switches or valves to open or close, move funds from one account to another, or convey a military order almost as quickly over thousands of miles as it can from next door, and just as easily from a terrorist hideout as from an office cubicle or military command center.[24] A computer message from Earth can steer a vehicle and point a camera on the surface of Mars; a false or malicious computer message can traverse multiple national borders, leaping from jurisdiction to jurisdiction to avoid identification, complicate lawful pursuit, or escape retribution.[25]

Those studying the issues raised by the information revolution have faced as an initial quandary the problem of acceptably defining the concept of information warfare.[26] Additionally, the term is loosely used to refer to in lieu of or in addition to

---

[22] *Id.* at 7.

[23] *See* CRITICAL FOUNDATIONS *supra* note 9 at 7; REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON INFORMATION WARFARE – DEFENSE (*hereinafter* Defense Science Board report), Office of the Under Secretary of Defense for Acquisition & Technology (November 1996) at 3.

[24] CRITICAL FOUNDATIONS *supra* note 9 at 7.

[25] *Id.*

[26] Aldrich, *supra* note 4, at 6.

this term like infowar, netwar, and command and control war.[27] Others define information warfare as an electronic conflict in which information is a strategic asset worthy of conquest or destruction.[28]

> The current DOD definition of information warfare is:
>
> Actions taken to achieve information superiority by affecting an adversary's information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.[29]

Information systems are the organization, collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual; in information warfare, this includes the entire infrastructure, organizations, and components that collect, process, store, transmit, display, and disseminate information.[30]

These concepts are best understood by examining a few prominent "cyber-attacks" perpetrated by individuals and by organizations in the recent past. In 1995, a Russian student in St. Petersburg accessed the Citibank database 40 different times and gained entry to Citibank's cash management system. With access to the bank's daily transfers of over $500 billion, he was able to transfer more than $12 million to a

---

[27] *Id.* at 2.

[28] *Id.*

[29] Chairman, Joint Chiefs of Staff Instruction 3210.01, *Joint Information Warfare Policy*, of January 1996; *See* Science Applications International Corp., *Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance* (2d ed. July 1996)(*hereinafter* SAIC Report).

[30] SAIC Report, *supra* note 29.

private account until he was arrested.[31] In New York, 2 individuals used a scanner on a windowsill to steal over 80 thousand cellular telephone numbers from motorists driving along a Brooklyn highway and used those telephone numbers for about $1.5 million per day in fraudulent phone calls.[32] A disgruntled employee of Sun Microsystems penetrated Air Force computers and allegedly retrieved air tasking orders that delineated military targets in the event of a real-life conflict.[33]

Not surprisingly, organized groups have availed themselves of the benefits of information warfare. The doomsday cult in Japan that launched a Sarin nerve gas attack in the Tokyo subway broke into the mainframe of Mitsubishi Heavy Industries as part of an effort to arm itself with laser weapons.[34] The United Nations was victimized by a group of cyber-bandits when 4 of its computers containing all of the data concerning human rights violations in Croatia were stolen; the theft dealt a heavy blow to the U.N.'s efforts to prosecute war crimes.[35] Finally, banks in London, New York, and Tokyo paid over $500 million to cyber-terrorists who demonstrated to the banks an ability to bring their respective computer operations to a grinding halt.[36]

---

[31] Timothy L. Thomas, *Deterring Information Warfare: A New Strategic Challenge*, in PARAMETERS, Winter 1996-1997, at 81.

[32] Richard Power, CURRENT AND FUTURE DANGER: A COMPUTER SECURITY INSTITUTE PRIMER ON COMPUTER CRIME AND INFORMATION WARFARE (Computer Security Institute 1996) at 29.

[33] Winn Schwartau, INFORMATION WARFARE AND CYBER-TERRORISM: PROTECTING YOUR PERSONAL SECURITY IN THE ELECTRONIC AGE (2d ed. 1996).

[34] Power *supra* note 32 at 20.

[35] *Id.* at 24.

[36] Martin C. Libicki, *Defending Cyberspace and Other Metaphors*, 23, (Center for Advanced Concepts and Technologies, National Defense University 1997).

However one might define information warfare, it is now possible for a Hindu fanatic in Hyderabad or a Muslim radical in Madras, or even a deranged "geek" in Denver, to cause immense damage to people, cities, or, with some effort, to armies 10,000 miles away.[37] Whatever or whoever the origin of the threat, it can be classified into two broad types of threat: the ability to manipulate perceptions, emotions, interests, and choices through the use of telecommunications and the speed with which information assaults can be conducted, giving crisis managers little time to respond.[38]

In a well-known study, DOD concluded in 1995 that its unclassified computer systems had been accessed without authorization over 250,000 times; out of this number, only 5% of the users knew of the improper access and, of that number, only 2% made a report of it.[39] Top officials in the U.S. government have stated that information warfare presents the swiftest growing threat to national security.[40]

On the other hand, several commentators have suggested the threat may not be as real as intimated. A major information attack against the U.S. military, for example, is statistically improbable, although it does not mean that an attack against some parts of the national security apparatus or the economic interests of the U.S. is

---

[37] Schwartau, *supra* note 33 at 398.

[38] Thomas, *supra* note 31 at 85.

[39] Libicki, *supra* note 36 at 25; Schwartau *supra* note 33 at 20.

[40] The Director of Central Intelligence, John Deutsch, said that hacker attacks present the second greatest threat to national security after weapons of mass destruction; the Deputy Attorney General, Jamie Gorelick, believes that information warfare is the nation's premier security threat. Libicki *supra* note 36 at 9; John Deutsch, *Terrorism*, FOREIGN POLICY, Sep. 22, 1997 (Carnegie Endowment for International Peace).

unlikely.[41] While it is unlikely as well that a state would employ only information-based attacks in attempting to conquer another state, information warfare will be critically important in creating the "fog of war" that produces an atmosphere of disorientation that then enables conventional forces to seize the opportunity of invasion.[42] Additionally, it would be extremely difficult to completely block the functioning of the NII to the point where it equates to a war-time blockade, but, conversely, for a state that has grown so dependent on information flow, an attack aimed at main points of information distribution could resemble a physical economic blockade.[43]

Despite the differences among commentators about the likelihood of an information attack and its scope, declarations by states undoubtedly proclaim their assessments of the size of the threat. Russia, for instance, has declared that the use of information warfare against Russia or her armed forces would categorically not be considered a non-military phase of a conflict, whether casualties result or not, and Russia retains the right to use nuclear weapons against the means and forces of such an information attack.[44]

C. Methods of Information Warfare

To understand how the laws concerning the use of force may apply to this developing area of warfare, it will be helpful to know how this concept may actually

---

[41] Schwartau, *supra* note 33 at 371.

[42] Libicki, *supra* note 36 at 28-29.

[43] Libicki, *supra* note 36 at 67-72.

[44] Thomas, *supra* note 31 at 82.

be implemented. Aside from the description of some consummated attacks listed above, information warfare can be conducted in the following ways:

Command and control, the ability to generate commands and communicate with deployed forces is disrupted;

Electronic warfare, degrading or disrupting the flow of electrons of information;

Intelligence-based warfare, the integration of sensors, emittors, and processes into reconnaissance, surveillance, target acquisition, and bomb damage assessment systems;

Psychological operations, actions to affect the perception, intentions, and orientation of a decision-maker;

Cyberwar, the use of information systems against virtual personnas or groups;

Hacker-warriors, persons who destroy, degrade, exploit, and compromise information systems; and

Economic warfare, use of information systems to create an information blockade.[45]

These attacks can generally be carried out by corrupting the hardware or software in a system; using an insider with access to an information system; external hacking; or flooding the system with incoming calls or requests for data.[46] Additionally, an info-warrior can insert a virus into a telephone-switching system;

---

[45] Thomas, *supra* note 31 at 83, citing Libicki, *What Is Information Warfare*, Center for Advanced Concepts and Technology (National Defense University 1995).

[46] Libicki, *supra* note 36 at 15, 17; Greg Rattray, *The Emerging Global Information Infrastructure and National Security*, 21-FALL Fletcher F. World Aff. 81, 84 (1997).

implant logic bombs set to detonate at a predetermined time and disrupt, for example, rail line switching grids; or simply access a message distribution system and transmit a phony message.[47]

A new kind of weapon is being refined – the computer malicious code (CMC).[48] CMCs are software that intentionally cause undesired and unpredictable consequences when inserted inside computers or networks.[49] Typical CMCs are viruses, as described above; worms, which self-replicates itself and overloads the power of a computer; trojan horses, which copies information that is later used by a hacker to gain entry to an otherwise secure system; logic bombs, which sit inside software until a predetermined detonation time; and trap doors, which allow undetectable entry into a network.[50]

How these new methods of warfare can be used was the subject of a study by the RAND Corporation for DOD. Using its conventional, "The Day After . . .," scenario-based exercise model, RAND presented senior members of the DOD and the intelligence communities an exercise involving a conflict between Iran and the U.S. in the Persian Gulf area.[51] The exercise concluded that a coordinated series of seemingly random information attacks on different communications, logistics, and

---

[47] Douglas Waller, *Onward Cyber Soldiers*, Time Magazine, August 21, 1995, Vol. 146, No. 8.

[48] Lorenzo Valeri, *Guarding Against A New Digital Enemy*, Jane's Intelligence Review, August 1, 1997.

[49] *Id.*

[50] *Id.*

[51] RAND Report, *supra* note 1.

transportation links in the U.S. would seriously inhibit the ability to respond to a swift conventional invasion on the Saudi Arabian peninsula.[52]

D. Emerging Issues

The background materials should indicate there are prominent issues in the application of international law to information warfare as a method of fighting wars. There is general agreement that, in information warfare, there are no front lines and traditional territorial boundaries are blurred.[53] Determining state responsibility for an attack will be extremely difficult since attacks are largely anonymous, and tracking down perpetrators of an attack is very hard to do.[54]

State sovereignty and territoriality face grave challenges from information warfare. Through sovereignty, a state combines the intangible idea of a people with the tangible construct of a political and economic entity.[55] Statehood is characterized by the exercise of sovereignty, which is best understood in terms of political and economic control.[56] Ironically, the very technology which has linked the world's states by telecommunications may render states' laws, framed in terms of power over their territory, inconvenient or irrelevant in many ways.[57]

---

[52] *Id.*

[53] *Id.*; Thomas, *supra* note 31 at 84.

[54] Libicki, *supra* note 36 at 49-51.

[55] Douglas H. Dearth & R. Thomas Goodden, CYBERWAR: SECURITY, STRATEGY AND CONFLICT IN THE INFORMATION AGE 277 (AFCEA International Press 1996).

[56] Alexander D. Roth, *The Struggle for Coherent International Regulatory Policy*, in TOWARDS A LAW OF GLOBAL COMMUNICATIONS NETWORKS *supra* note 8, at 339.

[57] Organization for Economic Cooperation and Development, AN EXPLORATION OF LEGAL ISSUES IN INFORMATION AND COMMUNICATION 12 (Paris 1983).

In this uncertain environment, the stage is thus set to determine whether the traditional laws concerning the use of force can be applied to information warfare or whether new rules will need to be developed.

II. DISCUSSION

A. Limitations on the Use of Force

From the beginning of modern international law in the mid-seventeenth century through World War II, a state's unilateral use of force as a matter of its conduct of foreign relations was a legitimate exercise of its discretion.[58] Following World War II, though, the United Nations Charter imposed an agreed prohibition on the unilateral use of force by states. Articles 2(3) and 2(4) of the Charter were viewed as the two most important declarations of states, weary of a twentieth century filled through its midpoint with unprecedented carnage and violence, to formally and finally outlaw war as an instrument of foreign policy and interstate relations.

> Article 2(3) provides: All members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.
>
> Article 2(4) provides: All members shall refrain in their international relations from the threat or use of force against the territorial integrity or

---

[58] Mark W. Janus & John E. Noyes, INTERNATIONAL LAW: CASES AND COMMENTARY (West 1997).

political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

These two provisions were seen by most observers as the heart of the Charter and the two most important principles of modern international law.[59] States thereby accepted the obligation to settle all disputes by peaceful means and to refrain from the use or threat of use of force in their international relations.[60]

The Charter framework permitted only two exceptions to this otherwise total ban on the unilateral use of force: force used in self-defense against an armed attack,[61] or when authorized by the Security Council to restore or maintain international peace and security.[62] Thus, the Charter does not outlaw all demonstrable uses of force, particularly for credible reasons of self-defense, but it does carefully circumscribe when forced may be used.[63]

As such, nations agreed after World War II that peace was the paramount value, and that grievances and sincere concern for "national security" or other vital

---

[59] Oscar Schachter, *The Right of States to Use Armed Force*, 82 Mich. L. Rev. 1620 (1984).

[60] *Id.*

[61] Article 51, U.N. Charter, provides: Nothing in this Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.

[62] Articles 39 and 42, U.N. Charter. Article 39 provides: The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security. Article 41 provides for measures not involving the use of armed force that the Security Council may authorize. Article 42 provides: Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security.

[63] David J. Scheffer, *The Great Debate of the 1980s, in* RIGHT V. MIGHT: INTERNATIONAL LAW AND THE USE OF FORCE 1, 4 (Council on Foreign Relations 1989).

interests would not authorize the start of a war.[64] Future wars could thus only be justified as a war against an initial aggressor – in self-defense by the victim, in collective self-defense of the victim by others, or by all.[65]

1. The meaning of "force" in Article 2(4).

Article 2(4) has admitted to much ambiguity over the last 50 years as states have urged particular exceptions to it when particular uses of force have not neatly fit into the actual Charter exceptions.[66] Indeed, some scholars have questioned whether Article 2(4) is so vague and uncertain that a state might plausibly justify any use of force it chooses to exercise.[67]

One ambiguity is whether Article 2(4) prohibits the use of force if not intended as a matter of conquest. That is, some suggest that the prohibition applies only to force designed to deprive another state of its territory, while others suggest that the proscription includes any force that violates territorial borders, however temporarily and for whatever purpose.[68] Professor Henkin argues that the answer is revealed in the way states behave in acting to prohibit or condemn armed aggression:

---

[64] Louis Henkin, *The Use of Force: Law and U.S. Policy* in RIGHT V. MIGHT 37, *supra* note 63.

[65] *Id.*

[66] Although beyond the scope of this paper to discuss these suggested exceptions in detail, they are worth mentioning particularly in light of the U.N.'s proclivity since the end of the Cold War to enlarge the uses of force in the name of maintaining world peace and security. Those exceptions include use of force for humanitarian intervention; to support self-determination; to intervene in the name of socialism; and to restore or institute democratic government. Henkin, *supra* note 63; W. Michael Reisman, *Criteria for the Lawful Use of Force in International Law*, 10 Yale Journal of International Law 279 (1985).

[67] Schachter, *supra* note 59 at 1621; *see also* John F. Murphy, *Force and Arms in* UNITED NATIONS LEGAL ORDER 247-318 (Oscar Schachter & Christopher Joyner ed. 1995).

invasion, attack, or occupation (however temporarily); sending armed bands or mercenaries to another country; bombing; blocking ports; and attacking other forces wherever they may be located, are all prohibited uses of force.[69]

Another ambiguity in Article 2(4), and one most critical to the idea of information warfare, is what acts constitute a use of force. The concept of force is itself ambiguous and is susceptible of a broad and a narrow reading.[70] In the broad sense, force includes all types of coercion, whether they be physical, psychological, financial, political, or economical.[71]

When the Charter was drafted, the subcommittee assigned to construct Article 2(4) considered whether the prohibition on the use of force should include measures short of armed attacks such as economic or psychological measures. The subcommittee, after extensive consideration, rejected the inclusion of economic measures in the meaning of Article 2(4) and, consequently, Article 2(4) was generally understood to apply only to armed force.[72]

The work of the International Committee of the Red Cross that led in 1949 to the signing of the four Geneva Conventions[73] lent support to the view that Article 2(4) applied only to actual armed intervention by one state into another state's territory. According to the rapporteur for those Conventions, Jean Pictet, those

---

[68] Henkin, *supra* note 63 at 39.

[69] Henkin, *supra* note 63 at 41.

[70] Schachter, *supra* note 59 at 1624.

[71] *Id.*

[72] Belatchew Asrat, *Prohibition of Force Under the U.N. Charter: A Study of Article 2(4)*, (Iustus Forlag, Sweden 1991).

[73] These Conventions will be discussed in more detail, *infra*.

Conventions were meant to apply to any difference between two states leading to the intervention in one state by another state's armed forces.[74] This view certainly supported the idea that Article 2(4) only limited the crossing of an international border by one state's military forces. As such, at least in the early days of the Charter, the defining characteristic of prohibited "force" seemed to be that of physical confrontations.[75]

One writer has suggested that force is anything that compels a state to take a decision or action it otherwise would not have taken or done.[76] Under this view, a state would commit an act of force if its state-controlled automobile manufacturer dumped a fleet of underpriced cars into a foreign market and that foreign state had to enact trade barriers to protect its domestic producers. More pertinently, under this view, a state which had to take action to ensure network security because of unauthorized entry into its information systems by elements of another state could consider that intrusion an act of force and be permitted to respond in kind. This intrusion, though, would lack the physical aspects of what states ordinarily understand to be manifested in a demonstration of force. While the intrusion would undoubtedly be unlawful, the question would be whether it is unlawful because it is

---

[74] Aldrich, *supra* note 4, at 7.

[75] *Id.*; *See* Henkin, *supra* note 63 at 47-49; Professor Henkin notes that the International Court of Justice in the case that Nicaragua brought against the United States for its role in mining Nicaraguan ports and assisting the Contra rebellion against the Sandinista government, tried to give more clarity to the meaning of what qualifies as force by concluding that assistance provided to the contras in Honduras was a use of force by the United States against Nicaragua even though U.S. personnel did not take part directly or physically in the conflict. Professor Henkin adds that this conclusion was diluted when the ICJ concluded that Nicaragua's assistance to Sandinistas attempting to overthrow the government of El Salvador did not qualify as a use of force against that country.

[76] Aldrich, *supra* note 4, at 7.

the improper use of force or for some other reason. It is readily apparent that information warfare will not lend itself easily to considerations of "physicality" in assessing whether it constitutes force.

2. Aggression.

The General Assembly has tried to inform the meaning of the term "force" by qualifying it in terms of aggression. Obviously due to the experience of World War II and the Nuremburg trials where a "war of aggression" was found to be a war crime, the United Nations has implicitly equated "force" with aggression.[77] As with the efforts to define the limits of "force" in Article 2(4), the General Assembly's work in defining the term "aggression" split into two views: newly independent states saw the term as including all types of coercion, whether by armed attacks or by economic, political, or psychological coercion; Western states interpreted the term restrictively and generally rejected a broad interpretation.[78] Ultimately, the General Assembly limited the definition of aggression to those acts having physical attributes of assaulting another state's territory, that is, armed military intervention, albeit for whatever reason.[79]

---

[77] *See* Benjamin B. Ferencz, DEFINING INTERNATIONAL AGGRESSION: THE SEARCH FOR WORLD PEACE (Dobbs Ferry N.Y. 1975) for a general discussion of the General Assembly's development of the Resolution defining aggression.

[78] Aldrich, *supra* note 4 at 13.

[79] Kanuck, *supra* note 5, at 288-289; "Aggression is the use of armed force by a State against the sovereignty, territorial integrity, or political independence of another State[.]" Resolution on the Definition of Aggression, art. 1, G.A. Res. 3314, U.N. GAOR, 29th Sess., Supp. No. 31, at 143 U.N. Doc. A/9890 (1974).

The Resolution on Aggression contains a nonexclusive list of examples of acts constituting aggression, including:

Invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary;

Bombardment by the armed forces of a State against another State's territory;

Blockage of ports or coasts by the armed forces; and,

An attack by one State's armed forces against another State's armed forces.[80]

One can possibly construe this Resolution as still being ambiguous and not providing concrete limits on information warfare. For example, one writer concludes that it is not possible to equate a naval blockade, which the Resolution prohibits, and an information embargo by denying one state access to its own information systems.[81] A U.S. Navy international law expert was quoted as wondering, "When does manipulation of information qualify as a use of force? Somewhere along the spectrum which ranges from the broadcasting of T.V. Marti or Radio Free Europe to the physical destruction of foreign communications facilities, the line of force is crossed, but I do not believe we know where that line is yet."[82]

It may be that information warfare will produce a reexamination of the limits on aggression advanced by developing states and focus on the economic and

---

[80] Resolution on Aggression, *supra* note 79, art. 3.

[81] Kanuck, *supra* note 5, at 289.

[82] *Id.* at 288-289, quoting Captain David Peace, who, at the time, was head of the Navy's international law division. Ultimately, the meaning of aggression is intertwined with the concepts of peaceful uses of the high seas and of outer space. A similar debate about the meaning of "peaceful" uses of those areas has developed, and, in each instance, state custom has defined this term as permitting military uses of those areas that are not "aggressive." For a more detailed discussion of "peaceful purposes," *see* sections IIC6 and IIE, *infra*.

psychological threats posed by this new medium of warfare. Conversely, since such a review would likely still focus on the status of the actors and the purpose of an information attack, it is not likely that the Resolution would be amended in the near future.

3. State practice.

Rather than search only in multilateral treaties for limits on the use of information warfare, it will be instructive, in the view of Professor Schachter, to look to states' practice to determine whether a particular use of information warfare is a use of "force."[83] Additionally, it would be very instructive to examine the personnel involved in a particular action and the goal to be achieved through the action. In this respect, then, a customary understanding of the limits of information warfare should develop.

In this light, an information warfare "attack" directed by electronics technicians of a state's armed forces, at another state's vital services, like electrical power grids or telephone systems would more clearly represent an armed attack coming under the provisions of article 2(4) than one, for example, on purely economic systems like a state's stock market or national banking system.[84] As such, where data manipulations result in significant destructive effects that are

---

[83] *See* Schachter, *supra* note 59, at 1623. Professor Schachter, in discussing what acts qualify as force, advises that much can be drawn from the way states attempt to justify certain actions as permitted under the Charter. In this respect, by basing a particular action on, for example, article 51 of the Charter, a state implicitly acknowledges that the action under review is a use of force which, if not justified by article 51, would, therefore, be prohibited by article 2(4).

[84] Charles J. Dunlap, Jr., *Cyberattack! Are We At War?*, NCSA News (Nov. 1996), quoted in Hanseman, Robert G., *The Realities and Legalities of Information Warfare*, Air Force L. Rev. 173, 184 (1997).

indistinguishable in any meaningful way from those caused by traditional kinetic weapons, such assaults constitute "armed attacks" for purposes of article 51.[85]

Additionally, one should consider the efforts of various states to develop information warfare defense programs in determining what acts of information warfare might qualify as "force." By developing defenses for particular threats, states are implicitly concluding that such threats are potential uses of force against which it is necessary to defend. The only question then would be to determine the issue of state responsibility if some personnel other than that state's armed forces are involved in the particular means of information attack at issue.

In this respect, one might argue that information warfare is not included in the meaning of Article 2(4) since it does not involve an armed force entering into another state's territory. This nettlesome problem has indeed created conceptual difficulties in international law enforcement where scholars and legislators have struggled with ways to prescribe and enforce jurisdiction over cyber-criminals.[86] It is difficult to know whether an intrusion into one's information system represents the exuberance of a youthful hacker or a test of a state's destructive warfare capability; accordingly, distinctions between crime and warfare or accident and attack will be necessarily blurred.[87]

---

[85] *Id.*

[86] *See* e.g., Henry H. Perritt, *Jurisdiction in Cyberspace*, 41 Vill. L. Rev. 1 (1996); M. E. Bowman, *International Security in the Post-Cold War Era: Can International Law Truly Effect Global Political and Economic Stability? Is International Law Ready for the Information Age?*, 19 Fordham Int'l L. J. 1935 (1996); Rattray, *supra* note 46; Selin, *supra* note 14.

[87] Bowman, *supra* note 86, at 1942.

4. Intervention.

The United Nations added to the understanding of Article 2(4) when it began in the 1960's to consider the proliferation of newly independent states born from their former colonial forebearers. These states banded together to put on the General Assembly's agenda a number of issues meant to affirm their status as independent states and to limit the influence of the Cold War powers in manipulating the internal affairs of these new states. One result of these efforts was the resurrection of the notion that Article 2(4) should include non-armed force measures like economic or political coercion. Attempts to expand Article 2(4) were resisted but, nonetheless, the General Assembly did pass a significant resolution creating the Declaration on Intervention.[88]

Significantly, the Declaration on Intervention provides:

1. No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned;

2. No State may use or encourage the use of economic, political, or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive,

---

[88] Declaration on the Inadmissability of Intervention into the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, 20th Sess., Supp. No. 14 at 108, U.N. Doc. A/6014 (1965)(*hereinafter* the Declaration on Intervention).

terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State[.]

Thus, while the Declaration on Intervention undoubtedly would proscribe some types of information warfare, it does not do so as part of Article 2(4).[89]

5. Cooperation.

Another General Assembly Resolution provides another potential limit on the use of information warfare. In 1970, the General Assembly passed the Declaration on Friendly Relations[90] which reaffirmed the Declaration on Intervention and purported to restate existing customary law regarding the principle of nonintervention.[91] Like the Declaration on Intervention, this declaration serves to protect a state's territorial integrity and political independence from outside coercion. Each declaration contains broad statements about the type of outside influence that is prohibited. In cases where information warfare would plausibly not qualify as a use of force, these Declarations could still limit the use of information warfare in certain cases.

---

[89] *See* Kanuck, *supra* note 5, at 276. Mr. Kanuck mentions that the Declaration on Intervention is not part of Article 2(4) since that Article only speaks to "threat or use of force," but it is a part of the customary law attributes of state sovereignty. He also notes that what constitutes intervention, as with the use of force or aggression, is subject to disparately varying interpretations (essentially, the broad versus restrictive views common to the views of force and aggression) even though all states generally agree that intervention is illegal.

[90] Declaration on the Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance With the Charter of the United Nations, G.A Res. 2625, U.N. GAOR, 25th Sess., Supp. No. 28 at 121, 123, U.N. Doc. A/8028 (1970).

[91] David Wippman, *Change and Continuity in Legal Justifications for Military Interventions in Internal Conflict*, 27 Colum. Hum. Rts. L. Rev. 435, 445 (1996).

B. Self-Defense

1. Broad and narrow meanings.

Article 51 of the U.N. Charter permits the use of force in individual or collective self-defense against an armed attack. It was crafted as a way to ensure that a state in the post-Charter age did not have to become a hapless victim of an aggressor state that chose to ignore the Charter's prohibitions on the use of force.[92] A debate about the scope of self-defense has accompanied Article 51 almost from the onset of the Charter.

As with the scope of the content of Article 2(4), two main schools of thought about the meaning of Article 51 have arisen. One school, which interprets Article 51 strictly, limits the use of defensive force to those instances where an actual armed attack is occurring.[93] Under this reading, a state would have to try to exhaust all non-force, diplomatic means of resolving a dispute, and risk receiving the first wave of assault by an aggressor state, before being permitted to respond legally with force in kind.

The other school, which advocates an expansive reading of the Article, holds that the Charter did not eliminate the principles of self-defense as they were understood prior to the Charter, but, rather, the Charter merely reaffirmed the customary understanding of self-defense.[94] The customary understanding, which most scholars conclude was most appropriately voiced by Daniel Webster during the

---

[92] *See* Schachter *supra* note 59, at 1634-1635.

[93] Stuart G. Baker, *Comparing the 1993 U.S. Airstrike On Iraq to the 1986 Bombing of Libya: The New Interpretation of Article 51*, 24 Ga. J. Int'l & Comp. L. 99, 109 (1994).

[94] *Id.*

Caroline Incident, does not require a state to receive the first wave of assault before being permitted to reply in self-defense.[95] Nor does the *Caroline* standard require recourse to all available diplomatic means. Rather, the justification for the use of force is that there is no time or choice for any reasonable alternative other than using force because of the immediacy and certainty of the threat.[96]

The International Court of Justice in the *Nicaragua* case concluded that the Charter did not eliminate the customary understanding of self-defense.[97] It also concluded that the concept included the *Caroline* requirements of immediacy and absence of any reasonable alternative in limiting a response to a threat of attack.[98] The ICJ's opinion is strongly persuasive authority to conclude that the *Caroline* principle is embodied in Article 51. To date, though, the outer limits of the principle are not settled.

---

[95] Rex J. Zedalis, *Preliminary Thoughts on Some Unresolved Questions Involving the Law of Anticipatory Self-Defense*, 19 Case W. Res. J. Int'l L. 129, 173 (1987).

[96] Guy B. Roberts, *Self-Help In Combatting State-Sponsored Terrorism: Self-Defense and Peacetime Reprisals*, 19 Case W. Res. J. Int'l L. 243, 268 (1987). Advocates of the customary view of self-defense have spawned opposing camps on the limits of the *Caroline* standard as well because of the differences in understanding of the degree of immediacy of the threat. In short, the restrictive view of this standard is that the aggressor has to have his finger on the figurative trigger before force in self-defense may be employed, while those holding to a more liberal view of the term would employ force as the gun is being loaded and aimed. Zedalis, *supra* note 95, at 173.

[97] Oscar Schachter, *Self-Defense and the Rule of Law*, 83 Am. J. Int'l L. 259, 260-261 (1989); *see* Schachter, *Self-Judging Self-Defense*, 19 Case W. Res. J. Int'l L. 121 (1987); Henkin, *supra* note 63, at 47-49; *see also* Note, *Terror and the Law: The Unilateral Use of Force and the June 1993 Bombing of Baghdad*, 5 Duke J. Comp. & Int'l L. 457, 479 (1995).

[98] Schachter, *Self-Defense and the Rule of Law*, *supra* note 97, at 261.

2. Reprisal.

Closely related to self-defense is the concept of reprisal and its validity as an international custom in the post-Charter age. Reprisal was given its best pre-Charter expression in the arbitration between Germany and Portugal concerning the lawfulness of German military coercion against Portugal in Angola in 1914.[99] A reprisal, prior to the Charter, was permitted when: an offending state committed an act contrary to international law; the injured state must make a demand on the offending state and that demand goes unsatisfied; and the force used in the reprisal must be proportionate to the offending act.[100] Using this formulation, a state in committing reprisal could actually act in a way that was otherwise contrary to international law because of the inequity of the initial offensive and unredressed act.

Many hold that the Charter outlawed reprisal as a legitimate method for states to ensure their self-protection.[101] The *Corfu Channel* case is most often cited as the basis for this conclusion. In that case, the ICJ held that the United Kingdom violated Albania's territorial integrity by sailing into her territorial waters with the intent to retrieve naval contact mines that Albania had laid there to block international naval passage through the Corfu Channel.[102] Even though the British intended only to

---

[99] Naulilaa Incident Arbitration, Portuguese-German Arbitral Tribunal, 8 Trib. Arb. Mixtes 409, 2 R. Int'l Arb. Awards 1012 (1928), *discussed in* Rex J. Zedalis, *On the Lawfulness of Forceful Remedies for Violations of Arms Control Agreements: "Star Wars" and Other Glimpses At The Future*, 18 N.Y.U. J. Int'l L. & Pol. 73, 116 (1985).

[100] *Id.*

[101] Roberts, *supra* note 96, at 282-285; Note, *Terror and the Law*, *supra* note 97, at 486.

[102] Roberts, *supra* note 96, at 276; *see* Corfu Channel Case (U.K. v. Alb.), 1949 ICJ Rep. 4.

retrieve these hazards to navigation to present as evidence of Albania's illegal acts, the ICJ condemned the British for committing an unlawful reprisal.[103]

The view that reprisals have been outlawed in the post-Charter world finds support in those uses of force that have resembled reprisals but were presented as cases of self-defense pursuant to Article 51. The most notable examples of such uses of force were the U.S. attack on Libya in 1986 after the Berlin nightclub bombings and the Israeli incursion into southern Lebanon in 1982 to strike at terrorist groups that had harbored themselves there. More recently, the U.S. airstrike on Iraq in 1993 after the aborted assassination attempt on former-President Bush in Kuwait was, likewise, defended as an act under Article 51. The significant point of each of these incidents was the care with which each was defended as a matter of self-defense and not as a vaguely legitimate reprisal. Thus, it well could be that the practice of states has been to recognize the illegitimacy of reprisal and to implicitly recognize an obligation to try to justify a use of force as a defensive measure under Article 51.[104]

The concept of collective self-defense, when applicable, has not had as controversial a record of understanding in the Charter. Typically, the use of force in collective self-defense has been justified only in those cases where a victim state has actually requested assistance from a third state.[105] This has been so even in those cases where a collective self-defense treaty may arguably have permitted a third

---

[103] Schachter, *supra* note 59, at 1626; 1949 ICJ Rep. at 35.

[104] *See* Schachter, *supra* note 59, at 1626-1627; Jordan J. Paust, *Responding Lawfully to International Terrorism: The Use of Force Abroad*, 8 Whittier L. Rev. 711 (1986).

[105] Henkin, *supra* note 63, at 47-49; Schachter, *supra* note 97 at 271-273; *see* Schachter, *United Nations Law in the Gulf Conflict*, 85 Am. J. Int'l L. 452, 457 (1991); *Case Involving Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. U.S.), 1986 ICJ Rep. 14, 105.

party's use of force even when not requested to do so by a victim state.[106] More troubling cases have been when a state has tried to justify an act as one of individual self-defense when the facts and circumstances surrounding a case have indicated the situation really was one of purported collective self-defense, albeit there was no official request for assistance from a victim state.[107]

The initial hurdle in applying these concepts to information warfare is to consider whether a particular information attack qualifies as an armed attack. Presumably, if it does so qualify, then the victim state is entitled under the Charter to respond proportionately to the attack. Conversely, if the initial information attack is not seen as a use of force, then the "victim" state would risk, whether in responding in kind or through a more conventional attack, being branded as an aggressor in violation of Article 2(4). At the very least, the putative victim state would risk running afoul of the Declarations on Friendly Relations and Intervention if the initial attack was not seen as a use of force or a threat of force.

Assuming that a defensive reply is permitted, the issue of what would constitute a proportionate response, in terms of a commensurate information attack, is raised.[108] If the attack is already consummated by, for example, a virus that infected a

---

[106] *See* Henkin, *supra* note 63, at 47; 1986 ICJ Rep. 14, 105 (even existence of regional collective defense treaty did not obviate need for victim state to request assistance).

[107] In the *Nicaragua* case, the ICJ pointedly held that the U.S. could not justify its actions in Nicaragua as ones in individual self-defense. 1986 ICJ Rep. 14, 106; *see generally*, Nikolai Krylov, *Humanitarian Intervention: Pros and Cons*, 17 Loy. L.A. Int'l & Comp. L. J. 365 (1995); George P. Politakis, *From Action Stations to Action: U.S. Naval Deployment, "Non-Belligerency," and "Defensive Reprisals" in the Final Year of the Iran-Iraq War*, 25 Ocean Dev. & Int'l L. 31 (1994).

[108] As stated previously, it is presumed that replies such as a conventional airstrike or other actions involving an obvious use of force would be clearly governed by Article 51. The task here is to assess the application of Article 51 to a response based solely on pure information warfare. Additionally, a response combining pure information warfare tactics and more conventional tactics would, likewise, be

particular network, does this permit the victim state to launch a similar virus aimed at a network of the offending state? Alternatively, is the victim state limited in this instance to ridding its network of the virus and lodging a diplomatic protest? To complicate matters, if the victim state is not limited in its defensive response to a response in kind, could a victim state launch a larger information attack against the offending state as a way to repel subsequent information attacks?

Certainly, a mirror-image response, when a defensive reply is permitted, has never been required. If this were the case, then the purpose permitting force in self-defense (to repel the attack) would be severely undermined. This is because the initiating state would have no incentive to discontinue its attack if it knew that international law permitted only a tit-for-tat escalation of a conflict. The right to self-defense includes, then, the right to use sufficient force to repel the attack and not simply to stall it or even just to stop it. Accordingly, it would not be reasonable to hold that a victim state could only reply in kind to an act of armed force.[109]

The real question will be where the virus or the logic bomb or the Trojan horse has already been identified and measures to cleanse the information system attacked have been taken. That is, the issue would be whether an additional attack on the aggressor state is permitted. Does this scenario look more like the case where two Iranian gunboats have released their missiles at a surface vessel in the Persian Gulf and turned away to return to port (in which case there is arguably no right to engage those units with force) or does it look more like the case where the terrorist group has

---

more easily reviewed under Article 51 since the primary focus on such a response would necessarily be based on the conventional tactics. The information warfare component of such a combined response would in all likelihood not receive much critical analysis.

strafed the Rome and Vienna airports, bombed the nightclub in Berlin, and are preparing a new, imminent attack?

The question, of course, begs the answer. The simple fact that weapons were released will not normally be the only information available to an on-scene commander. Rather, he will have intelligence reports to supplement his battlespace awareness that will inform him about the degree of the threat he faces. He will also have awareness of the events leading up to a particular attack in terms of the political situation at hand, the parties likely to present a threat, their degree of sophistication, and other factors, all of which will bear on a decision to act in self-defense. In short, the more an information attack looks more like a concerted, strategic strike, based on all available pieces of information, the more likely the right of self-defense will arise.

3. Hot pursuit.

The customary right of hot pursuit permits a state to pursue into international areas one who committed a crime in the territory of that state. Pursuit could continue unless and until the perpetrator entered his own territorial space of the territory of a third state.[110]

The difficulty here is when, if ever, a perpetrator, during the course of hot pursuit in cyberspace, crosses into the sanctuary of a home state or third state. Suppose a foreign intruder in a network was detected and that intruder began to "escape" before his electronic capture. The architecture of the information

---

[109] Roberts, *supra* note 96, at 272-273.

[110] This customary principle has been set forth in Article 111, United Nations Convention on the Law of the Sea, Dec. 10, 1982, U.N. Doc. A/CONF.62.122.

infrastructure could complicate legal replies to the illegal intrusion. As mentioned earlier, the information infrastructure is not really a highway with clearly defined routes from point A to point B. Rather, it is an amalgam of servers, connections, telecommunications lines, personal computers, and other hardware and software where often the path from point A to point B never follows the same course. Instead, it "gets there" by the most electronically convenient means available at that particular time. Thus, the victim state has little way of knowing through purely information-based pursuit that he will be following the same path as the perpetrator nor that any responsive actions will not intrude on the territory, if it exists, of some third state.

In this respect, the 1986 airstrike against Libya is instructive for any similar extraterritorial reply against an information warfare aggressor. In that instance, American bombers based in England were denied permission by France and Spain to overfly those countries on the way to bombing Colonel Quaddaffi's headquarters in Libya.[111] The planes, instead, had to fly over the eastern Atlantic Ocean then through the airspace over the Strait of Gibraltor.[112] Assuming there could be some claims of territoriality laid on the segments of the information infrastructure, an aggrieved state could find itself with little protection if it had to obtain the consent of a number of other nations to pass through their "territories" on the way to completing an otherwise lawful act of self-defense against an aggressor state.

---

[111] Baker, *supra* note 93, at 105.

4. Proportionality.

In using defensive force, a state must ensure it uses only force proportionate to the force to be countered. Suppose, for example, there was reliable evidence that the simultaneous "downing" of the eastern seaboard's telephone systems and the New England electrical power grid were tied to the efforts of a rogue state and there was credible evidence that this group was about to launch a similar attack on the Midwest as part of an effort to sow confusion in the United States while planning for a more conventional assault on the country.

Assuming these acts could be viewed as aggressive attacks, assume next that the only way to block the next wave of information attack would be to infect the rogue state's electrical system with a virus. This action would have the effect of cutting off all power to the country's hospitals, the irrigation system, and the refrigerants needed to maintain essential medicines at an acceptable level. As a result, civilian deaths would surely result. Because of the redundancy of systems in the United States, disruptions to essential services and financial networks from the initial attack would be severely disrupted but only a minimum of American lives would likely be lost.

A detailed discussion of the aspects of proportionality and necessity in the law of armed conflict will be discussed further in this paper, in section IIC4 and 5, *infra*, but the issue bears raising now as it relates to self-defense. Obviously, the technology available to either side to a conflict will raise nettlesome questions about what is proper and what is not once the use of force in self-defense is permitted.

---

[112] *Id.*

At present, much of this discussion about proactive forms of information warfare in self-defense may be premature. Discussions to date about the national security aspects of information warfare defense have focused on network security and contingency plans in the event of significant network disruptions caused by information attacks.[113] Little attention has been given to the prospects of "offensive" information warfare acts of self-defense. What focus that has been made is cloaked in classified programs at the Pentagon.[114]

5. Armed attack.

Information warfare raises the chance to examine whether the focus of Article 51 should be changed from "armed attack" to a term that more realistically accommodates the threat posed by information warfare. It is illogical to concede that an electronic attack could have potentially more devastating and widespread consequences on a state than a terrorist's truck bomb yet refuse legitimate acts of self-defense because the putative attack was not an "armed attack." Even replacing that term with "aggression" would not yield a satisfactory result since that term, too, is currently limited to "armed" aggression.

Conversely, it could be potentially destabilizing to come too quickly to redefining the terms when the scope of the information battlefield and its tactics are still too uncertain for quantification or qualification. There is definitely a ready

[113] *See* CRITICAL FOUNDATIONS, *supra* note 9.

[114] *See* Defense Science Board Report, *supra* note 23, at 10.

temptation to assume too much about the potential of information warfare as a means of warfare. It will probably not, in the views of some commentators, totally replace conventional forces and arms nor will wars of the future ever be fought entirely by computers.[115]

As such, to change the Charter too quickly would very likely result in unintended consequences. One readily apparent consequence is that the understanding of "force" and "aggression" might yet come to include non-military types of aggression like economic, psychological, or political coercion. It is believed that the 50-plus years of the Charter have shown that rejection of these concepts from the original understanding of "force" was a prudent and stabilizing decision. States are probably unwilling now, if they ever will be, to consider certain types of economic coercion to be a use of force that would justify military responses. Otherwise, then we are only steps away from coming full circle to the days of conquest and wars of national right that prevailed in the 17th and 18th centuries. Certainly, that is not a path down which many states should be willing to go.

To summarize, the use of information warfare in defense against an information attack will depend initially on whether that first attack is considered an armed attack. In certain cases, such a conclusion can be drawn. In that event, proportionate action in self-defense is permitted. If the responsive act will result in unintended damage, a balancing of interests would be necessary to determine whether the proposed reply should be undertaken.

---

[115] CRITICAL FOUNDATIONS, *supra* note 9, at 17-19; Defense Science Board Report, *supra* note 23, at section 2.0, p. 4; Libicki, *supra* note 36, at 28-29.

C. The Law of Armed Conflict

1. The Law of the Hague and the Law of Geneva.

One area of international law that has potentially the greatest bearing on the tactics employed in information warfare is the law of armed conflict. This law is contained in conventional and customary law. Some of the customary aspects of the law of armed conflict, such as self-defense and hot pursuit, have already been discussed. This section discusses more fully the law contained in what is conveniently referred to as the Law of the Hague and the Law of Geneva.

From the custom and usage of nations, these two bodies of law developed.[116] The law of the Hague governs the application and conduct of force and the legality of weapons.[117] The law of Geneva, on the other hand, has come to be known as "humanitarian law" because it regulates the use of force to reduce unnecessary suffering particularly among civilian nonparticipants to a conflict.[118]

The laws of the Hague and of Geneva can be briefly summarized in the following manner: the right of belligerents to adopt means of injuring the enemy is not unlimited; it is prohibited to launch attacks against the civilian population as such; distinctions must be made between combatants and noncombatants so that

---

[116] Ariane L. DeSaussure, *The Role of the Law of Armed Conflict During the Persian Gulf War: An Overview*, The Air Force Law Review, 41, 42 (1994); Judith G. Gardam, *Noncombatant Immunity and the Gulf Conflict*, 32 Va. J. Int'l L. 813, 816 (1992).

[117] DeSaussure, *supra* note 116, at 42; Gardam, *supra* note 116, at 816.

[118] DeSaussure, *supra* note 116, at 42; Gardam, *supra* note 116, at 816.

noncombatants be spared as much as possible.[119] These principles are stated and repeated in numerous conventions and declarations of the customary law of armed conflict, the most notable of which are the Hague Conventions of 1907,[120] the four Geneva Conventions of 1949,[121] and the 1977 Geneva Protocols I and II Additional to the Geneva Conventions of 1949.[122] Besides these conventional sources, the law of armed conflict is reflected in a great deal of customary international law as well.[123]

---

[119] J. Ashley Roach, *Missiles on Target: Targeting and Recent Developments in the Persian Gulf*, 31 Va. J. Int'l L. 593 (1991); Captain Roach notes that these three principles are part of the cornerstones of the customary law relating to armed conflict. They have been codified in Protocol I Additional to the Geneva Conventions of 1949, 1125 U.N.T.S. 3 (1979), reprinted in DOCUMENTS ON THE LAW OF WAR (A. Roberts and R. Guelff 2d ed. 1989)(*hereinafter* DOCUMENTS ON LAW OF WAR). The United States signed this Protocol but has not ratified it. The United States agrees that the Protocol is declaratory of customary international law. Roach, at FN 3; Francis V. Russo, *Targeting Theory in the Law of Naval Warfare*, Naval L. Rev. 1, 25-26 (1992): these principles can be stated more exactly as follows: (1) the right of a belligerent to adopt means of injuring the enemy are not unlimited; (2) only combatants and legitimate military objectives may be attacked; (3) force may only be used when required to achieve legitimate military objectives; (4) the impact on noncombatants and nonmilitary objectives must not be disproportionate to the value of the military objective; and (5) the infliction of civilian suffering and destruction not authorized under the principle of proportionality in number (4), above, and beyond which is operationally required to achieve a legitimate military objective is prohibited.

[120] The Second Hague Peace Conference in 1907 led to the conclusion of thirteen conventions (ten dealing with the laws of land and maritime war) and one declaration (relating to a particular method of conducting warfare). These conventions codified many customary principles of land and naval warfare and set the stage for the development of rules respecting aerial warfare. Many principles contained in these conventions were reiterated in the later Geneva Conventions of 1949 (hereinafter GC 1949) and the subsequent 1977 Protocols Additional. *See* DOCUMENTS ON LAW OF WAR, *supra* note 119, at 3; this book reprints each of the thirteen conventions. Hague Convention IV, Respecting the Laws and Customs of War on Land, has an Annex setting forth substantive regulations implementing the Convention. These Regulations are the authoritative substantive provisions of the Convention and their articles are often cited as articles of the Convention and not the Regulations.

[121] The 1949 Geneva diplomatic conference produced these four conventions, relating to wounded and sick; wounded, sick, and shipwrecked; prisoners of war; and protection of civilians. DOCUMENTS ON LAW OF WAR, *supra* note 119.

[122] These Protocols amplified the protection accorded to victims of international armed conflict and, for the first time, codified protections for victims on noninternational armed conflicts. *Id.*

[123] *Id.* at 4. The importance of customary law in the law of armed conflict is reflected in the 1907 Hague Conventions, each of which contains what is known as "the Martens Clause." This clause, likewise, contained in the 1949 Geneva Conventions, states that:

> Until a more complete code of the laws of war is issued, the high contracting Parties think it right to declare that in cases not included in the Regulations adopted by

The thrust of these principles is to attempt to make armed conflict more humane by minimizing unnecessary suffering either through direct armed attack or through the collateral effects of an armed attack.

Under these principles, only military objectives may be attacked.[124] Military objects are those objects which, by their nature, location, purpose or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack.[125]

Article 52 of Protocol I Additional limits the use of force against military objects as a means of providing general protection to civilian objects. Article 52.3 specifies that, "In case of doubt whether an object which is normally dedicated to civilian purposes, . . . is being used to make an effective contribution to military action, it shall be presumed not to be so used."[126] Thus, the law seeks to protect civilian objects by applying a presumption that they are not ordinarily used for military purposes.

---

them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilised nations, from the laws of humanity and the requirements of the public conscience.

[124] Roach, *supra* note 119, at 596.

[125] *Id.* at 596, quoting Art. 52 of Protocol I Additional.

[126] Article 52, Protocol I Additional.

2. Applicability

A threshold question is whether these laws of armed conflict even apply to information warfare. This raises again the question whether pure information warfare would be a use of armed force under article 2(4) of the U.N. Charter. The Hague Conventions apply in "war" while the Geneva Conventions generally apply in times of declared wars or during periods of international armed conflict.[127] The question, then, is whether use of pure information warfare could be considered "armed conflict."

At first blush, it may seem difficult to conclude that injecting a virus into an information system or planting a logic bomb into a computer chip equates to the use of precision guided missiles or the crossing of an armored division across a territorial frontier. Nonetheless, the Geneva rules, at least, did not concern themselves with such minute analysis. Rather, those rules focused on a broad interpretation of acts that could be considered to be part of an armed conflict. The Commentary of the 1949 Geneva Conventions indicated that:

> [a]ny difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place.[128]

---

[127] *See* Hague IV, art. 1; Hague IX, art. 1; GC 1949, common articles 2, 3.

[128] COMMENTARY ON THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 17-21 (Jean S. Pictet ed.); *see* W. Gary Sharp, *Protecting the Avatars of International Peace and Security*, 7 Duke J. Comp. & Int'l L. 93, 121 (1996).

Thus, the focus of the Geneva Conventions protections is two-fold: any difference between two states and any intervention of members of the armed forces. That the limitation on intervention is not described in terms of a traditional notion of an armed invasion or strategic bombing indicates the preference for the law of Geneva to be of a wide scope. Further, "any" difference between states apparently triggers the Geneva protections, so long as there is a causal connection between that difference and the intervention of members of the armed forces.

Whether states actually agree with such an interpretation according a broad scope to the law of Geneva probably matters little, since states' practice indicates that they do agree with such a view.[129] In the United States armed forces, for example, commanders and operational units are routinely briefed on the laws of armed conflict and their applicability to any situation potentially involving the use of force.[130]

Moreover, while much discussion recently in the development and implementation of information warfare has centered on the defensive, protective aspects of it, it cannot be denied that attention is also being paid to the offensive capabilities of the concept as well. In the United States, the offensive capability of information warfare is being studied in classified channels, so this article must necessarily remain at the theoretical level. Presumably, though, these studies are being conducted with the idea that the laws of armed conflict will apply to it.

Additionally, as a practical matter, it would be inconceivable for a state to argue that it is using its military forces to develop what functionally appears to be a

---

[129] *See* Schachter, *supra* note 97, at 273.

[130] *See* DeSaussure, *supra* note 116, at 58.

warfighting capability and then to deny that the laws of armed conflict do not apply to it. Again, much can be concluded from the manner in which states justify particular actions. In this area, it will be inconceivable to imagine a state, under these circumstances, suggesting that its armed forces are exempt in this area from the laws of armed conflict. As such, it can safely be concluded that the laws of the Hague and of Geneva will apply to information warfare.

3. Applicability of Additional Protocol I

The applicability of Additional Protocol I to the 1949 Geneva Conventions to any international armed conflict further scrambles the propriety of information warfare. Two of the main parties in the Persian Gulf War, the United States and the United Kingdom, signed the Protocol but have not yet ratified it. The reasons for not ratifying the Protocol were that it was perceived to untenably legitimize terrorist forces as "freedom fighters"; to inject a subjective component to the proportionality analysis where a military commander could be easily second guessed about the tactics used to destroy a legitimate military object; and to impose a presumption that an object was not of a military character if it appeared that targeting it would result in excessive civilian casualties.[131]

---

[131] DeSaussure, *supra* note 116, at 48-50; Gardam, *supra* note 116, at 826-827; Letter of Transmittal from President Ronald Reagan, Protocol II Additional to the 1949 Geneva Conventions, and Relating to the Protection of Victims of Non-International Armed Conflicts, S. Treaty Doc. No. 2, 100th Cong., 1st sess., at III (1987), reprinted in 81 Am. J. Int'l L. 910 (1987)(President Reagan forwarded Protocol II, which provided protections for civilian persons in armed conflicts not of an international character and recommended ratification but decided not to forward Protocol I for Senate consideration); Schachter, *supra* note 105, at 466, noting that the presumption in Protocol I in favor of classifying an object as a civilian object remains controversial because it encourages states to camouflage military operations in a protected enclave.

There is strong evidence to suggest, however, that the U.S. and U.K. acted in a way during the Gulf War that showed their acceptance of the Protocol I provisions. The planners of the air campaign against Iraq went to great lengths at different points to emphasize that target selection and airstrike missions were done in a way to minimize civilian casualties.[132]

Moreover, the U.S. Navy and Air Force, at least, in their field manuals on the laws of armed conflict, contain prescriptive provisions that mirror the language of articles 51 and 57 in the Protocol.[133] The U.S. Army field manual on the law of armed conflict, conversely, does not contain similar provisions,[134] and the official view of the Army is that Protocol I does not apply to U.S. military operations.[135] Rather, the Army's view is that proportionality is limited, not to the Protocol I requirements, but to the customary limitations that civilians not be targeted directly or negligently; excessive casualties among the civilian population does not render nugatory the legitimacy of the military character of an object nor the necessity to

---

[132] DeSaussure, *supra* note 116, at 59; A. P. V. Rogers, LAW ON THE BATTLEFIELD, 43, 45 (Manchester Univ. Press 1996)(noting that some legitimate military targets were not bombed because of the potentially excessive civilian toll).

[133] Naval Warfare Publication (NWP) 1-14M, *The Commander's Handbook on the Law of Naval Operations*, para. 8.1.2.1; Air Force Pamphlet (AFP) 110-31, *International Law – The Conduct of Armed Conflict and Air Operations*, para. 5-3; *accord* Francoise J. Hampson, *Proportionality and Necessity in the Gulf Conflict*, 86 Proc. Am. Soc. Int'l L. 45, 46-47 (1992).

[134] *See* Department of the Army Field Manual (FM) 27-10, *The Law of Land Warfare*. Note, though, that para. 41 of FM 27-10 provides that "[L]oss of life and damage to property must not be out of proportion to the military advantage to be gained."

[135] Gardam, *supra* note 116, at 830-831.

destroy it if it would provide a military advantage.[136] In short, military necessity, under this view, always overrides proportionality.[137]

Additionally, there is a sharp division of views that state behavior during the Gulf War indicated an acceptance of the Protocol I provisions on proportionality.[138] As such, it cannot confidently be said that state practice during that conflict showed that the provisions of Protocol I have acquired a customary status. Still, while the exact balancing calculus required by articles 51 and 57 of the Protocol may not be customary law, it is probably safe to conclude that states do take some account of the anticipated effects of an attack on the civilian population in deciding whether to proceed.[139] To that extent, then, there is at least the contours of a principle of proportionality that would restrain a commander from attacking even an undeniably military object.

For information warfare, the problems raised by this issue will be in the targeting of those dual use systems which serve as a vital resource for the civilian

---

[136] *Id*; *see also* W. Hays Parks, *Air Warfare and the Law of War*, 32 A.F.L. Rev. 1 (1990). Professor Gardam also notes that another point of disagreement about Protocol I is that some consider the proportionality requirement to apply only to the overall conduct of a conflict and not to the discrete component airstrikes or infantry assaults of that conflict. Gardam, *supra* note 116, at 831.

[137] *Contra* DeSaussure, *supra* note 116, at 48 (noting that necessity emphatically does not override the humanitarian aspects of the laws of armed conflict and quoting Jean Pictet, the International Committee of the Red Cross Commentator for the 1949 Geneva Conventions that the humanitarian rules are peremptory norms).

[138] Gardam, *Proportionality and Force in International Law*, 87 Am. J. Int'l L. 381, 408-410 (1993) and *supra* note 116, at 834-835; Fritz Kalshoven, remarks to American Society of International Law, *Implementing Limitations on the Use of Force: The Doctrine of Proportionality and Necessity*, 86 Proceedings Am. Soc. Int'l L. 40, 41-42 (1992)(Protocol I did not apply); Hampson, *supra* note 133, at 45-47 and Schachter, *supra* note 105 at, 465-466 (Protocol I did apply).

[139] Again, there is evidence from the Gulf War air campaign that certain military objects were not bombed because of concerns for the impact on civilians nearby. *E.g.*, Rogers, *supra* note 132, at 43, 45 (switching stations and not generating stations in Iraq's electrical power grid were attacked to permit quicker post-War recovery of power; dams or other water supplies were not attacked for fear of flooding civilians).

population as well as retaining an undoubted military utility. It remains to be seen whether states will continue to officially abide by Additional Protocol I but, as a practical matter, seem to honor the Protocol more in ignoring it.

4. Necessity

The concept of necessity has long been a cornerstone of the laws of armed conflict. First stated conventionally in the 1856 Paris Declaration and the 1868 St. Petersburg Declaration, the essence of necessity is that only military objectives may be targeted.[140] Resorting to Additional Protocol I, military objectives are those objects, which, by their nature, location, purpose or use, effectively contribute to the enemy's war-fighting or war-sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage under the circumstances at the time of the attack.[141]

It is not difficult to confuse this concept with the requirement of proportionality. Proportionality involves an excessive number of noncombatant casualties resulting from an attack on an unquestionably military object; necessity, on the other hand, concerns the cumulative impact of attacks against particular targets which renders their characterization as a military object questionable.[142]

---

[140] *See* DOCUMENTS ON LAW OF WAR, *supra* note 119; Gardam, *supra* note 138, at 397.

[141] Article 52, Protocol I Additional; Roach, *supra* note 119, at 596.

[142] Hampson, *supra* note 133, at 46. Professor Hampson notes that there is an overlap in the two principles. She characterizes the issue of attacking Iraqi bridges during the Persian Gulf War as one of proportionality because of the number of civilian casualties resulting from those airstrikes; she concludes that the attacks on the Iraqi electrical power system, because of the long-term effects they had on the civilian population of Iraq, is a question of proportionality. Having made that distinction, it is relatively easy to not see the subtle difference in the two principles.

Where necessity will be at issue in information warfare will be against those systems or resources that have a dual use capability among a state's military forces and its civilian population. Such systems will be those integrally connected to or supporting power systems, communications lines, logistics and other supply networks.

The experience of the coalition forces in the Persian Gulf War is instructive in determining the application of the principle of necessity to information warfare. During that conflict, coalition forces targeted and repeatedly bombed objects that served the needs of the Iraqi armed forces but also the civilian population: oil storage sites; power stations and factories; railways, bridges, airports and ports used for the deployment of military forces and the movement of supplies.[143]

The targets in information warfare are likely to include communications and electrical power circuits. These broad categories of targets can subdivided into more discrete categories such as local or wide area military communications networks; switching stations for rail transportation; air traffic controller networks; and port facility communication networks. Potential targets could possibly include a state's financial network database or telephone cable-based communications system.[144] These targets might be strained to apply the concept of necessity.

A comparison to the law of naval warfare is instructive in determining the lawfulness of targeting a dual use information system. Any vessel, other than a warship, owned or operated by a belligerent possesses military character, regardless

[143] Rogers, *supra* note 132, at 41-42.

[144] One study noted that over 95% of the Department of Defense telecommunications network is based on shared-use civilian systems. Rattray, *supra* note 46, at 82.

of whether it is operating under a neutral flag or bears neutral markings.[145] That is, any neutral vessel acquires enemy character and may be treated by a belligerent as an enemy warship when engaged in the following acts: taking a direct part in the hostilities on the side of the enemy; or acting in any capacity as an auxiliary to the enemy's armed forces.[146]

Acquiring military character, then, depends on the degree of control exercised over the object and, more essentially, the importance of the object to the warfighting effort. Aside from the obvious military objectives like enemy warships and aircraft, proper military objectives to include in targeting include lines of communication and other objects used to conduct or support military advantage.[147]

Similarly, capabilities that are not exclusively used for military purposes may nonetheless be targeted if those capabilities or facilities indirectly but effectively support and sustain the enemy's war-fighting ability.[148] On this basis, for example, the Union's destruction of Confederate cotton fields during the Civil War was lawful because the Confederacy used profits from the sale of cotton to fund its arms purchases.[149]

Likewise, the oil transportation systems of Iraq and Iran during their war in the 1980's were legitimate military targets because each side used profits from the

---

[145] NWP 1-14M, *supra* note 133, para. 7.5.

[146] *Id.* para. 7.5.1.

[147] Roach, *supra* note 119, at 596.

[148] *Id.*

[149] *Id.*

sale of their oil to fund their respective war-fighting capabilities.[150] Specifically, Iran financed almost all of its war effort through sales of its oil; Iraq targeted merchant vessels carrying Iranian oil that were sailing in exclusion zones publicly declared by Iraq to be zones in which it would target vessels suspected of carrying Iranian oil.[151] As these Iraqi attacks on otherwise neutral vessels were aimed at interfering with Iran's war-sustaining capability, these merchant vessels acquired the character of Iran and, thus, were lawful targets under the law of armed conflict.[152]

With these points in mind, the initial focus would be whether the information system to be targeted has acquired enemy character. It may acquire this character if controlled by the opponent or if serving any capacity as an auxiliary to its war efforts. Another way of stating this is to determine whether the information system so effectively contributes to the opponent's war-fighting or war-sustaining capability such that its destruction or disablement would constitute a definite military advantage under the circumstances. If so, it may then be targeted. If not, it may not be targeted.

In this respect, attacks on a state's financial network, that is, the national stock market exchange, if any, and connections to banking facilities, might arguably be justified. Although a seemingly non-military objective, this information system could become a legitimate target if, but only if, there was some real connection between it and the state's war-sustaining effort. Without such a connection, there would be no

---

[150] *Id.* at 597.

[151] *Id.* at 603.

[152] *Id.* at 604.

military advantage obtained by attacking such a system and, therefore, such an attack would be unlawful.

Similarly, an attack on the telecommunications network of an opponent could be justified if that network is used in command and control functions or for supply and personnel transportation. Again, the focus at this point is not on the shared-use nature of a system, but, instead, solely on its utility to the war effort.

The difficult question would be whether the connections of that network to other nations or to multinational corporations involved in that network, or simply the presence of more civilian beneficiaries in that information system, would change the analysis. It is tempting to leap quickly and conclude that the analysis would be changed. That is likely to be the case, but, if so, it will not be because the information system is not a military object. Rather, it will be because the attack on such a system would result in a disproportionate effect on non-military components and persons in that system. As such, it would be more appropriate to consider this question under the rubric of proportionality.

5. Proportionality

Because proportionality, whether under Protocol I or under a customary law articulation, necessarily involves a balancing of civilian lives and property against military benefit, this part of information warfare will garner the most difficult analysis. As

to the law of armed conflict generally, the principle of proportionality is a conundrum that has probably never been, nor ever will be, solved.[153]

Reference to the Persian Gulf War is once again instructive in assessing the parameters of this concept. If anything, that war showed the difficulty in applying the principles of discrimination and proportionality because of the commingling of military and civilian targets.[154] The coalition forces destroyed Iraq's electrical power grid and targeted several bridges among other targets. The power system was used, in addition to its military function, to power the nation's water supply and irrigation systems, refrigerate medicines, and provide power to hospitals and homes. The destruction inflicted on the Iraqi civilian population was undeniable.[155] This was so even though there were undoubted military advantages to targeting these systems.[156]

Because of the collateral devastation wreaked on these military objectives, the coalition was sharply criticized for its perceived failure to take account of those

---

[153] Schachter, *Implementing Limitations on the Use of Force: The Doctrine of Proportionality and Necessity*, 86 Proc. Am. Soc. Int'l L. 39 (1992)("Centuries of discussions by philosophers and jurists about the meaning of the concepts of proportionality and necessity in human affairs do not seem to have produced general definitions capable of answering concrete issues.").

[154] Schachter, *supra* note 105, at 466. Professor Schachter concluded that, as the coalition forces destroyed most of the means of modern life support in Iraq by bombing her power plants, bridges, roads, and communications facilities, the standards for discrimination and proportionality had little practical effect in the conduct of the war.

[155] J. W. Crawford, *The Law of Noncombatant Immunity and the Targeting of National Electrical Power Systems*, 21-FALL Fletcher F. World Aff. 101, 110 (1997), noting that an estimated 70,000 civilian deaths resulted directly from the bombing during the air campaign and indirectly from the effects of the loss of most of the nation's power generating system. The loss of power resulted in decreased hospital capacity, spoilage of essential vaccines and other medicines, loss in agriculture output because of failed irrigation systems, and increase in disease from loss of power to purify and distribute water.

[156] For example, the power system supported the storage of suspected biological and chemical munitions; computer-integrated anti-aircraft systems; fuel pumping facilities used for trucks, tanks, and aircraft; and loading bombs and other explosive agents. Crawford, *supra* note 155, at 109; Kalshoven, *supra* note 138, at 42-43 (bridges were legitimate targets as conduits of military supplies).

collateral effects.[157] Indeed, some have suggested that the experience in the Gulf War shows that targeting decisions must go beyond considering the "direct" collateral effects of an attack and consider also the long-term indirect effects.[158]

Additionally, assuming Protocol I applies, a military commander is required by Protocol I to make a determination that the military advantage to be gained by targeting the commercial satellite outweighs the collateral or incidental damage to the civilian population.[159] The Protocol prohibits the indiscriminate attack of civilians, and indiscriminate attacks include those which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[160]

Article 51.5 provides:

> Among others, the following types of attacks are to be considered as indiscriminate:
>
> (a) an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and

[157] *See, e.g.*, Schachter, *supra* note 105, at 452; Rogers, *supra* note 132, at 42-43.

[158] Crawford, *supra* note 155, at 111, 114; Hampson, *supra* note 133, at 47, 50-51; Gardam, *supra* note 116, at 813-815, 828.

[159] Roach, *supra* note 119, at 597; Crawford, *supra* note 155, at 107.

[160] Crawford, *supra* note 155, at 107.

(b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[161]

In this respect, a lawful attack on a military objective could be deemed illegal because of its indiscriminate effect on a civilian population. This outcome would ensue because the benefits gained by the attack would be outweighed by the harm caused, even indirectly, to the civilian population. Essentially, this is the argument of those who criticized some of the coalition targeting decisions in the Gulf War.

An attack on a particular communications satellite could, for example, have catastrophic, albeit unintended, collateral effects. It is nearly beyond debate that communications and information links are essential to the proper ordering of daily life. The growing dependency of states on the benefits provided by different types of satellites has probably changed the equation for assessing what is indiscriminate effect. A nation's reliance on satellites for internal and international communications, agricultural assessments, resource location, and flood management and other environmental protection could provide a basis to conclude that the loss of the ability to tap these benefits would constitute an impermissible collateral effect.

A civilian population without an essential telecommunications network wrought by its destruction could have devastating consequences in health care, financial security, commerce, agricultural output, and, potentially, maintaining

[161] Art. 51.5, Protocol I Additional.

various life-sustaining processes. It is not too far-fetched to think that the loss of a navigational satellite system could result in an untimely delivery of medicines and essential foodstuffs. Protocol I Additional prohibits attacks which render useless objects indispensable to the survival of the civilian population.[162]

In addition, the law prohibits indiscriminate attacks, that is, ones that either directly or negligently target civilians. This proscription is found in Protocol I as well as customary law. This limitation could affect the method of information warfare chosen for a mission. For example, a logic bomb is planted into a computer's circuitry and then "activated" at some later time. It would be an indiscriminate attack to plant a logic bomb in a computer or a network without some reasonably confident idea where that bomb would be activated. If a state simply let loose a logic bomb not knowing what foreign information system it would detonate in, then, arguably, such a tactic would violate the rule against discrimination.

Likewise, any other method of information warfare that would not have a reasonably predictable field or scope of destructive application would be prohibited by this principle. Thus, a virus could potentially be forbidden as a means of information warfare since a virus by its "nature" propagates without limitation to infect whatever system to which it is provided access. A virus could be proscribed, then, if there is a reasonable certainty that the foreign defense ministry's network, which was the primary focus of the virus, would provide the virus access, even indirectly, to its civilian telecommunications network.

[162] Article 54, Protocol I Additional.

Another troubling issue would be the type and duration of warfare selected. If, to gain the desired military advantage, one is not required to destroy the targeted military object, then the laws of armed conflict forbid using force that is more than necessary. One justification for the continued bombing of the Iraqi electrical system, even though it was neutralized early in the air campaign, was to prevent Iraq from restoring its system and, thereby, its war-fighting ability.[163] The question here would be whether a particular method of information warfare would be too much force in relation to the desired end. That is, if a state can effectively disrupt communications lines by flooding the telecommunications circuits with simultaneous dialings, should it be limited from using a method that has longer-lasting detrimental effects?

During the Gulf War, the coalition used precision guided missiles that purportedly avoided a great amount of unnecessary collateral destruction. This raised the question whether the states were then obligated to use these missiles in all airstrikes.[164] The consensus appears to be that states were not so required, but probably because the number of these missiles in the overall arsenal was not significant.[165] Also, the need to assure protection for the coalition forces permitted them not to have to rely entirely on the precision munitions.

Nonetheless, in information warfare, if a state could conceivably strike an information system with an electronic means of attack as opposed to a conventional airstrike, the question exists whether the state would be obliged to do so if doing so

---

[163] Crawford, *supra* note 155, at 108-109.

[164] Adam Roberts, *The Laws of War: Problems of Implementation in Contemporary Conflicts*, 6 Duke J. Comp. & Int'l L. 11, 20 (1995).

[165] *Id.*

results in significantly less collateral damage. At this stage in the development of information warfare, and in light of the Gulf War-PGM experience, we are probably not yet at that stage. Warfare could, however, progress to that point where such non-lethal, precision strikes may be required by the customs of warfare over less precise, more destructive methods.

6. Neutrality

The concept of neutrality in war emerged with the early development of international maritime law.[166] Maritime states sought to resist belligerents' interference with neutral maritime trade during the 18th and 19th centuries, and the law of neutrality developed through custom as a result.[167] Neutrality emerged from the Hague 1907 Conventions as the subject of two different treaties concerning neutrality in case of war on land (Hague V) and at sea (Hague XIII).[168] In each convention, the theme for neutrality was of impartiality. That is, neutral powers had the right to not become the target of either belligerent but had the duty to ensure that neither belligerent seized an advantage from either the neutral state or its citizens.[169] A state lost its neutrality if it assisted one of the belligerents in any manner and not the other or permitted its citizens to likewise assist one of the belligerents to the other's

[166] DOCUMENTS ON LAW OF WAR, *supra* note 119, at 61.

[167] *Id.*

[168] *Id.* 61, 109.

[169] *Id.* 61-62, 109.

exclusion.[170] Thus, the principal right of neutrality is inviolability of territorial integrity while the principal duties of neutrality are abstention and impartiality.[171]

A principal purpose of the law of neutrality is to protect neutral commerce. Neutral commerce involves all commerce between a neutral state and another neutral state not involving materials of war or armaments destined for a belligerent, and all commerce between a neutral and a belligerent that does not involve the carriage of contraband or otherwise sustain the belligerent's war-fighting capability.[172] As mentioned, above, a neutral power can acquire enemy character, and become a legitimate target, if it, *inter alia*, operates directly under enemy control, orders, charter, employment, or direction.[173]

Given the type of architecture used in the world's interconnected information systems, the question of neutrality in information warfare includes the issue of whether a state loses its neutrality by not preventing a belligerent from using, for example, its telecommunications system in conducting information warfare.[174] Likewise, the risk faced by a civilian company based in a neutral state of becoming a

---

[170] Articles 5 and 9, Hague V, which provide: A Neutral Power must not allow [belligerents to move troops or war materials across its territory; permit belligerents to erect communications stations or use existing stations for purely military communications] and apply impartially to each side any restrictions the neutral Power imposes and ensure its citizens do not violate this impartiality; Articles 6 and 9, Hague XIII provide: the supplying of a belligerent with of war materials is prohibited; restrictions against belligerents must be applied impartially.

[171] NWP 1-14M, *supra* note 133, para. 7.2; AFP 110-31, *supra* note 133, para. 2.6; FM 27-10, *supra* note 134, para. 512.

[172] NWP 1-14M, *supra* note 133, para. 7.4; David L. Peace, *Neutrality, The Rights of Shipping, and the Use of Force in The Persian Gulf War*, 82 Proc. Am. Soc. Int'l L. 146, 147-149 (1988).

[173] Roach *supra* note 119, at 598-599; NWP 1-14M, *supra* note 133, para. 7.5.2; Todd A. Wynkoop, *The Use of Force Against Third Party Neutrals to Enforce Economic Sanctions Against a Belligerent*, 42 Naval L. Rev. 91 (1995).

[174] The issue will also include whether use of a third party's satellite makes that satellite a legitimate non-neutral target. That issue will be discussed more fully, *infra*.

target will also be raised. Another issue will be whether a belligerent can conceivably cross through a neutral power's "cyber" territory on its way to attacking the other side to a conflict.

As to the first question, neither of the Hague neutrality conventions does not obligates a neutral state to prevent a belligerent from using its communications apparatus.[175] Similarly, a neutral state is not obliged to prevent its citizens from sharing private communications facilities with belligerents, again, so long as impartiality is observed.[176] Thus, a neutral state would not lose its neutrality if it permitted each side to a conflict access to a locally-based civilian Internet Service Provider.

The more difficult question is whether a neutral's territory can be violated by a belligerent's computer virus happening to pass through that state's information system network because of the machinations in the belligerent state's router. Put differently, are there neutral zones in cyberspace? The answer could depend on whether a state can claim sovereignty over different components of the global information infrastructure. Presumably, a state must have some territory over which to claim neutrality. Conversely, information warfare could expand the notion of neutrality to the point where the principle is violated if the state causes some impact on any area other than its own by some aggressive act. In this respect, it would not matter what course an information attack takes over the GII. It is sufficient that it

---

[175] Hague V, Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, article 8; Hague XIII, Concerning the Rights and Duties of Neutral Powers in Naval War, article 9.

[176] Hague V, article 9; Hague XIII, article 9.

courses over some parts of it other than that state's and the receiving state's parts of the GII.

There will be a practical problem in ensuring neutrality in information systems. The best way to ensure neutrality would be for a neutral state to impose blocks on access to its information systems rather than insist that belligerents stay away. Doing this, though, may risk that state losing equally neutral communications and connections from other neutral states. This would probably be too high a price, so, the more likely outcome will be that neutral states will not impede access to its information systems by any party to a conflict.

Should cyberspace become an internationally protected zone, similar to outer space or the high seas?[177] This question would be similar to the one facing international scholars since the dawn of Sputnik regarding the delimitation of outer space and territorial airspace.[178] As a result of the shock wave that Sputnik sent through the international legal system, the United Nations created the Committee on Peaceful Uses of Outer Space.[179] That Committee drafted the Principles on the Use of Outer Space[180] which served as the cornerstone for the Outer Space Treaty.[181] The Outer Space Treaty provided that outer space is the common heritage of mankind and,

---

[177] *See* John Kish, INTERNATIONAL LAW AND ESPIONAGE 102-109 (David Turns ed. 1995)(the legal regime of international spaces is governed by their common international status and, hence, claims to sovereignty are not honored).

[178] *Id.* at 115-116.

[179] Rita Lauria White & Harold M. White, Jr., THE LAW AND REGULATION OF INTERNATIONAL SPACE COMMUNICATION 235 (Artech House, Inc. Norwood MA 1988).

[180] U.N. Gen. Ass. Res. 1348 (XIII).

[181] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 18 UST 2410, TIAS 6347 (1967). This treaty and its application to information warfare will be discussed in more detail *infra*.

as such, would be used only for peaceful purposes and the common benefit of mankind.[182]

Similarly, the United Nations through the years has sponsored several initiatives to codify the customary law of the sea. In 1982, the Third United Nations Conference on the Law of the Sea produced a comprehensive treaty regarding the ocean spaces and the attendant rights and duties of states in, under, and over those spaces.[183] UNCLOS provides for the division of the oceans into discrete spaces and, as one goes further from the landmass of a coastal state, lessening rights of sovereignty over those spaces.[184] Ultimately, the oceans become the high seas, which, like outer space, are the common heritage of mankind, and over which no state may lay a claim of sovereignty.[185]

Conversely, in the other major technological development of this century, the birth of aircraft, states faced the choice of treating the airspace above its territory as free, international spaces like the high seas or as restricted national areas similar to its landmasses and internal waters. Eventually, in the Chicago Convention of 1944,[186]

---

[182] Outer Space Treaty, articles I, II.

[183] Law of the Sea Convention, *supra* note 110.

[184] UNCLOS divides the ocean spaces into internal waters and the territorial sea, over which a state generally has complete sovereignty (art. 2); a contiguous zone, over which a state has rights to enforce laws relating to fiscal, immigration, sanitation, and customs matters (art. 33); an exclusive economic zone, over which a state has rights to regulate the exploitation and conservation of resources (art. 56); and the high seas, over which no state has a right to exercise its sovereignty (arts. 87-89).

[185] UNCLOS, article 87-89. Article 87 sets forth a nonexclusive listing of high seas freedoms, including the rights of navigation and overflight of the high seas; article 88 reserves the high seas solely for peaceful purposes; and article 89 invalidates any claim of sovereignty over any part of the high seas. Additionally, Article 90 provides that every state has the right to navigate on the high seas.

[186] Convention on International Civil Aviation, 61 Stat. 1180, TIAS 1591, 15 UNTS 295.

they chose to apply notions of territoriality to the airspace above its territory and grant limited and conditional rights of entry into those airspaces.[187]

It is probably too early in the development of the technology of cyberspace and issues that will result from this development, for example, as it concerns the commission of domestic criminal offenses, to try to identify neutral or international spaces in cyberspace.[188] A more prudent course would be to allow that part of the law to develop further and then proceed from there to solving this issue. By enacting and implementing domestic criminal laws for acts committed in cyberspace, states are showing an intention to treat certain parts of the global information infrastructure as sovereign territory. As such, the resolution of the "neutrality" and sovereignty over cyberspace will probably follow the course of national airspace as reflected in the Chicago Convention. As such, it is unlikely that a "common heritage" portion of cyberspace, similar to outer space or the high seas, will be carved out. Consequently, the notion of neutrality will probably continue to exist in the uses of cyberspace and information warfare.

7. Ruses and Perfidy.

Another challenge to the application of traditional notions of the laws concerning the use of force and armed conflict will be in the area of ruses and perfidy or the law of chivalry. The law of armed conflict permits deceiving the enemy

---

[187] Article 1 of the Chicago Convention provides that states have complete and exclusive sovereignty over the airspace above its territory; article 5 sets forth the conditions for the use of national airspace by foreign civil aviation, essentially conditioned on permission of that state.

[188] *E.g.*, Perritt, *supra* note 86; *see* Johnson & Post, *supra* note 21, regarding the development of the law of merchants, *lex mercatoria*, in response to the inability of the local laws of princes and lords to resolve disputes that arose during the course of trade between merchants over states' borders.

through stratagems and ruses of war to mislead him, to deter him from taking action, or to induce him to act recklessly, provided the ruses do not violate rules of international law applicable to armed conflict.[189] The law, however, forbids the resort to treacherous means to kill or injure the enemy, and this is called perfidy.[190] These principles have attained customary status and are restated in Hague Convention IV and in Additional Protocol I.[191]

The Regulations to Hague IV provide at article 23 that it is forbidden to kill or wound treacherously or to make improper use of a flag of truce, or of the national flag or of the military insignia and uniform of the enemy.[192] Hague IV described these means as examples of treacherous acts, but perfidy was not further defined.

Additional Protocol I, however, defined perfidy as acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.[193] Examples of perfidy under this definition include the feigning of surrender or truce; feigning of incapacitation by wounds or sickness; feigning of civilian, non-combatant status; feigning of protected status through use of signs unique to the United Nations or neutral or other states not party to the

---

[189] J. Ashley Roach, *Ruses and Perfidy: Deception During Armed Conflict*, 23 Univ. Toledo L. Rev. 395 (1992), quoting D. Schindler and J. Toman, THE LAWS OF ARMED CONFLICT 3 (3d ed. 1988).

[190] NWP 1-14M, *supra* note 133, para. 12.1.2.

[191] *Id.*; Hague IV Regulations, arts. 23, 24; Additional Protocol I, art. 37(2).

[192] Hague IV Regulations, art. 23.

[193] Additional Protocol I, art. 37(1).

conflict.[194] The emphasis in Additional Protocol I, then, is to reinforce the protections afforded to the different classes of persons addressed in the four 1949 Geneva Conventions.

Whether the principles of ruse and perfidy will limit particular methods of information warfare may be assessed by examining the types of warfare permitted and not permitted under these principles. The obvious examples would be methods that abuse the symbols of protected organizations, neutral states or states not party to the conflict. For example, it would probably be perfidy to attempt access to an enemy's information system to inject a virus under the guise of an electronic communication emanating from the United Nations or using a domain name suggesting the origin of the communication was from a neutral country.

A more complicated issue, though, would be if such a communication was launched under the guise of the enemy country or used a domain name suggesting the communication originated in the enemy country. In land and naval war, it is permissible to use enemy uniforms, markings or flags to deceive the enemy, so long as the true colors are displayed prior to an engagement.[195] The rules for aircraft prohibit using enemy markings at any time under the reasoning that, once airborne, an aircraft cannot readily change its markings like ground troops or a naval vessel can.[196]

This presents the question whether a disguised communication is more like war on land and at sea, or like war in the air, or something different. Reviewing ruses that have been deemed acceptable may help in determining the answer. Permitted

---

[194] *Id.*

[195] Roach, *supra* note 189 at 414.

deceptions include false intelligence information, electronic deceptions, and use of enemy codes, passwords, and countersigns.[197] Some commentators suggest the prohibition in Additional Protocol I against the use of emblems, insignia or uniforms refers only to concrete visual targets and not to signals and codes.[198] This view of the limits on using enemy emblems, insignia or uniforms is implemented on the U.S. services' handbooks on the laws concerning armed conflict.[199]

It would appear, based on these examples, that disguising a communication to inject a virus into an information system would not be improper since it is simply using enemy codes or signals. One could reasonably argue, though, that the disguised communication is more properly like the mismarked aircraft and, particularly when the system to be infected is used for civilian purposes along with the military use, it would be perfidious to cripple the non-military component of that system.

The former view is very likely to be the acceptable view among states. The counter-argument actually goes more to necessity and proportionality than it does to perfidy. This is because the ruse employed does not invite the possible wrongful abuse of or damage to a protected status under the Geneva Conventions. Accordingly, such uses of information warfare will not necessarily be limited by the law concerning ruses and perfidy.

---

[196] *Id.*, 414-415.

[197] *Id.* at 398.

[198] Roach, *supra* note 189 at 398.; M. Bothe, K. Partsch & W. Solf, NEW RULES FOR VICTIMS OF ARMED CONFLICT, 1-603 (1982) at 214.

[199] NWP 1-14M, *supra* note 133, para. 12.5; FM 27-10, *supra* note 134, para. 51; AFP 110-31, *supra* note 133, para. 8-4.

8. Espionage.[200]

Another aspect of the law of armed conflict that may impact on information warfare is the law concerning espionage. Traditionally, a spy is any person who acts clandestinely or under false pretenses and obtains, or attempts to obtain, information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.[201]

Although the Hague Rules do not condition the acts of a spy on intrusion into another state's territory, customary law has traditionally limited acts of espionage to acts occurring within the territory of the state that is the subject of the acts of spying.[202] As such, customary law permits a state to forbid others from photographing strategic objects and events taking place within its territory.[203]

---

[200] This section will address acts of espionage and not the status of persons as spies during wartime and their treatment after capture as spies or prisoners of war.

[201] Hague IV Regulations, article 29. This 1907 formulation was based on previous customary declarations about the attributes of a spy. In the United States, an early definition of a spy was found in the 1863 Lieber Code, at article 88, which defined a spy as a person who secretly, in disguise or under false pretenses, seeks information with the intent of communicating it to the enemy. Instructions for the Government of the Armies of the United States in the Field, prepared by Francis Lieber, promulgated as General Orders No. 100 by President Lincoln, 24 April 1863, as a code of conduct for Union soldiers during the Civil War.

[202] Kish, *supra* note 177 at 83 (fundamental legal status of national territory determines the general principles governing espionage in those areas) and 97-101 (inviolability of national airspace is established in customary and conventional law); Quincy Wright, *Espionage and the Doctrine of Nonintervention in Internal Affairs*, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, 12 (Roland J. Stanger ed. 1962)(*hereinafter* ESSAYS ON ESPIONAGE)(peacetime espionage, and any penetration of state territory in violation of local law, violates the international law duty to respect the territorial integrity and political independence of other states).

[203] Richard A. Falk, *Space Espionage and World Order: A Consideration of the Samos-Midas Program*, 52, in ESSAYS ON ESPIONAGE, *supra* note 202.

Conversely, the ICJ effectively held in *The Corfu Channel Case*[204] that a maritime state had the right to engage in strategic observation in the course of conducting innocent passage through a coastal state's territorial waters.[205]

From this follows the corollary that observation from international spaces, like the high seas or the airspace over the high seas, is not prohibited by international law.[206] Satellite observation and remote sensing from outer space of sovereign territories has long been considered an acceptable state practice.[207]

This view was implicitly suggested by the United States after the Soviet Union shot down the U-2 pilot, Gary Powers, during his ill-fated reconnaissance flight over the Soviet Union in 1960. The United States admitted responsibility for improperly intruding into Soviet airspace, but did not admit to conducting espionage operations.[208] The international community thought little of this stance by the United States, and, consequently, implicitly affirmed the notion that physical presence in foreign territory is a prerequisite for spying. Accordingly, observation from areas outside the territory of a state should not be considered spying.

---

[204] 1949 ICJ Rep. 4.

[205] *Id.*; in that case, a British warship transiting Albania's territorial waters conducted observations of Albania's coastal defenses that were threatening to attack the British ship.

[206] Geoffrey B. DeMarest, *Espionage in International Law*, 24 Denv. J. Int'l L. & Pol'y 321, 335 (1996).

[207] *E.g.*, Youseff Sneifer, *The Implications of National Security Safeguards on the Commercialization of Remote Sensing Imagery*, 19 Seattle U. L. Rev. 539 (1996); Richard A. Morgan, *Military Use of Commercial Communications Satellites: A New Look at the Outer Space Treaty and 'Peaceful Purposes,'* 60 J. Air L. & Com. 237 (1994); Center for Research of Air and Space Law, SPACE ACTIVITIES AND EMERGING INTERNATIONAL LAW 404-406 (N. M. Matte ed. 1984).

[208] Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, 29-43, in ESSAYS ON ESPIONAGE, *supra* note 202. As several commentators have noted, there has long been a related question whether espionage is an act limited to times of armed conflict or if it can also be committed during peacetime. Professor Stone's comments were made in that context and were not meant to suggest that observations conducted in national airspace could not otherwise be considered spying.

Unresolved is whether this limitation extends only to international spaces or to any non-sovereign area including the territory from which the reconnaissance activity is conducted. The answer is important because, if an AWACS plane operating on the high seas in the Persian Gulf can permissibly monitor events inside one of the Gulf states, can a person at the National Security Agency (NSA) at Fort Meade, Maryland, permissibly monitor transmissions intercepted in cyberspace from that same Gulf state? If not, then the monitored state could claim an affront to its territorial integrity or political independence in violation of article 2(4) of the Charter.[209]

The Hague neutrality rules prohibit using neutral territory as a base of operations for spying.[210] These rules could be used to argue that the territorial limitation should be expansive, that is, clandestine operations from any non-international space should be prohibited. In this manner, the specialist at the NSA would be a spy. On the other hand, the neutrality rules were meant to reaffirm territorial integrity and to protect a neutral state, so they should not control the answer here.

Ultimately, there seems little reason not to treat the NSA analyst as a spy if that person actually is intruding into another state's territory. On the other hand, if the analyst is merely flying in cyberspace and "passively" intercepting emissions from another state, then he should not be considered a spy. Certainly, the answer will depend heavily on the result of trying to delimit cyberspace, if that will be possible.

---

[209] Whereas in the pre-Charter days, a state could have considered such an act to be an act of war. *See* NWP 1-14M, *supra* note 133, para. 12-8.

[210] Kish, *supra* note 177, at 128-129.

At the same time, it is possible to view current attempts to hack into a network as nothing other than spying. In such a case, however one views the architecture of the information infrastructure, a hacker is breaking into information system resources that are physically located in national territory. It really does not matter that the hacker travels through different way-stations in cyberspace. What counts is the ultimate action of intruding into mainframes or system resources that are unquestionably inside of a state. In this manner, focusing on where the information resides or where it is located when misappropriated confuses the simple fact that an intrusion into a defined area has taken place. Thus, assertive and proactive acts into identifiable resources inside of a state, rather than passive monitoring, should readily be treated as espionage.

D. International Telecommunications Law

It is probably a truism to say that telecommunication services, considered in their totality, form one of the key infrastructures of modern society.[211] The main international instrument concerning international telecommunication, the International Telecommunications Convention,[212] impacts on information warfare. There should not be much debate that the Convention will permit a state to take defensive action when threatened with information attacks. Indeed, the Convention reaffirms a state's essential right to defend itself and its citizens.

---

[211] Gerd D. Wallenstein, INTERNATIONAL TELECOMMUNICATIONS AGREEMENTS, Introduction at v, (Dobbs Ferry NY 1977).

[212] International Telecommunications Convention, Malaga-Torremolinos, of October 25, 1973, reprinted in Wallenstein *supra* note 211.

Article 18 of the Convention provides that the right of the public to correspond by means of the international service is recognized. In article 19(1), however, the member states of the Convention reserve the right to stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, to public order, or to decency, provided that the state immediately notifies the office of origin of the stoppage of any such telegram or any part thereof. The state may withhold notification if the security of the state would be placed in danger.

By article 19(2), member states further reserve the right to cut off any other private telecommunications which may present a danger to state security or be contrary to their laws, public decency, or public order. Moreover, states reserve the right to suspend the international telecommunications service for an indefinite time, either generally or for certain relations and for certain kinds of correspondence.

Applying these principles, states are permitted to employ measures like jamming frequencies in situations where extraterritorial transmissions disturb national airspace, threaten national security, or threaten domestic values.[213] As an example of the domestic implementation of the Convention, in the United States, the President is authorized by section 606 of the Communications Act of 1934[214] to exercise certain authority during a war or upon a proclamation that there exists a war or a threat of war, or a state of peril or other national emergency and suspend telecommunication

[213] TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS, *supra* note 8 at xii.

[214] Section 606 of the Communications Act of 1934, 47 U.S. Code sec. 606.

services within the United States and to use or control any radio or wire facility or station.

Thus, the Convention clearly permits a state under information attack to suspend or block the medium of transmitting those attacks. There would be no proscription against a state taking such protective measures, then, in the face of an actual or threatened attack whether it be from an opposing state or private source.[215]

Another important aspect of international telecommunications law is the requirement that the satellite networks on which telecommunications is based be used for peaceful purposes. INMARSAT[216] and INTELSAT,[217] international satellite organizations created by treaties, through their constitutive documents and internal legal opinions, have expressed their understanding of the principle.

INMARSAT provides maritime satellite services for communications and navigation. In the 1980's it concluded that its services could be used by warships during peacetime but, during hostilities, only for actions pursuant to U.N. resolutions and for purposes recognized by international humanitarian law like rescue of persons

---

[215] As will be discussed, there may be limitations in other constitutive organizations devoted to telecommunications.

[216] International Maritime Satellite Organization, *see* Morgan, *supra* note 207, at 281-286; Article 3 of INMARSAT Convention provides its basic purposes: (1) to make provision for the space segment necessary for improving maritime communications, and, as practicable, aeronautical communications [.]; (3) The Organization shall act exclusively for peaceful purposes.

[217] International Telecommunications Satellite Organization, *see* Morgan, *supra* note 207, at 289-293; article 3 of INTELSAT's basic document provides: [its purpose is to] continue . . . the design, development, construction, establishment, operation and maintenance of the space segment of the global commercial telecommunications satellite system[.] Its basic document does not provide that its services shall be used exclusively for peaceful purposes. It does, though, provide that the space segment may be used, on request, for "specialized telecommunications services" *other than for military purposes* (emphasis added).

or vessels in distress; aiding the sick and wounded; and other purposes related to navigational safety or distress.[218]

INTELSAT, meanwhile, provides commercial telecommunications satellite services. Its constitutive document provides that services may be used for "specialized telecommunications services, other than for military purposes." This provision has been interpreted only to proscribe the provision by INTELSAT of specially dedicated satellites for military use but not to prohibit military use of a satellite that already provides commercial satellite services.[219]

During the Persian Gulf War, INMARSAT and INTELSAT resources were used by each side in the conflict. The Director General of INMARSAT expressed concern that the U.S. Navy used its services impermissibly for nonpeaceful purposes while the U.S. maintained that the services were used in support of the U.N. resolutions which necessarily implied a peaceful purpose.[220] Nonetheless, the State Department advised the Director General that any planned INMARSAT usage beyond that in support of U.N. resolutions would be consistent with the INMARSAT Convention.[221] In so doing, the State Department seemed to indicate agreement with the Director General's position, but the State Department's reply to INMARSAT was fairly ambiguous because it did not directly concede agreement with the Director General's conclusions. It is thus unclear whether the U.S. shares this view of the limits of "peaceful purposes" held by INMARSAT.

---

[218] Morgan, *supra* note 207, at 286-288.

[219] *Id.* at 291-294.

[220] Morgan, *supra* note 207, at 295-296.

[221] *Id.*

INTELSAT has not disagreed with the view that militaries may use commercial services satellites to conduct military operations because such uses are not pursuant to a "specialized service" from INTELSAT.[222] Thus, it did not object to the use of its commercial service resources during the conflict.

This suggests that any aggressive type of information warfare would probably be unlawful under the INMARSAT and INTELSAT charters. Defensive information warfare would probably be unlawful under the INMARSAT charter unless premised on an internationally-recognized basis in favor of humanitarian principles. Under the INTELSAT charter, defensive information warfare would not be unlawful.

E. Space Law

The final area of substantive law to examine for the international limits on the use of information warfare as a means of conducting warfare is the law concerning outer space. The Magna Carta of outer space, so to speak,[223] is the Outer Space Treaty.[224] Article IV of the Outer Space Treaty provides that outer space will be reserved for peaceful purposes.[225] Although article IV only provides technically that the moon and celestial bodies shall be used for peaceful purposes, it has generally

---

[222] *Id.* at 294.

[223] Morgan, *supra* note 207, at 298.

[224] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, *supra* note 181.

[225] Article IV sets forth in pertinent part: The moon and other celestial bodies shall be used by all States Parties to the Treaty solely for peaceful purposes. The establishment of military bases, installations, and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited.

been accepted since the dawn of the space age that "outer space shall be used exclusively for peaceful purposes."[226] The question, then, is whether using space-bound assets like telecommunications satellites, or targeting such satellites, to facilitate information warfare is prohibited by the Outer Space Treaty.

Since the space age began in the 1950's, two schools of thought have arisen concerning the meaning of the peaceful purposes clause. One view is that "peaceful purposes" means nonmilitary actions.[227] The opposing view is that the term means nonaggressive actions. The United States has consistently held that "peaceful purposes" is limited to nonaggressive actions.[228] This view is based on reference to Article III of the Outer Space Treaty which provides that all space activities shall be in accordance with the U.N. Charter.[229] Because the Charter permits states to use force in self-defense, the term "peaceful purposes" must also permit the use of defensive force and only ban aggressive, offensive acts which are, likewise, banned by the Charter.[230]

Similarly, other parts of the Outer Space Treaty mention concepts like, "common interest of all mankind," "benefit of all peoples," "broad international cooperation," "maintaining peace and security," and "use in accordance with

---

[226] Bruce Hurwitz, THE LEGALITY OF SPACE MILITARIZATION 59 (1985); *see* Ralph G. Steinhardt, *Outer Space in* UNITED NATIONS LEGAL ORDER 766-769, *supra* note 67.

[227] S. Chandrashekar, *Problems of Definition: A View of an Emerging Space Power*, in PEACEFUL AND NON-PEACEFUL USES OF SPACE, PROBLEMS OF DEFINITION FOR THE PREVENTION OF AN ARMS RACE 81 (*hereinafter* PEACEFUL AND NON-PEACEFUL USES OF SPACE)(Bhupendra Jasani ed. 1991).

[228] Hurwitz, *supra* note 226 at 68.

[229] Kunich, *Planetary Defense: The Legality of Global Survival*, 41 A. F. L. Rev. 119, 133 (1997).

[230] *Id.*

international law," and provide a basis to support the "nonaggressive" interpretation.[231] On this basis, outer space is to be used in a cooperative way to benefit all peoples and in a manner which does not jeopardize international peace and security.[232] In this respect, the use of space for "aggressive" information warfare would be inconsistent with the Charter and, therefore, inconsistent with the Outer Space Treaty.

A reasonable argument can be made that, viewing solely the language of the Treaty, the nonmilitary interpretation of the clause is the correct one.[233] Quite simply, however, the drafters could have specifically provided for the exclusion of military uses of outer space but chose not to do so. Early on, the former Soviet Union espoused this view but quickly changed course after its military satellite program was, so to speak, launched and off the ground.[234] Thereafter, in applying the Outer Space Treaty, the United States and the former Soviet Union, as the preeminent space powers, consistently showed their understanding of the term "peaceful purposes" as meaning nonaggressive.[235] Significantly, no state has ever formally protested the United States interpretation of this clause.[236] Pursuant to the Vienna Convention on

---

[231] Morgan, *supra* note 207, at 302.

[232] *Id.*

[233] Ivan Vlasic, *The Legal Aspects of Peaceful and Non-Peaceful Uses of Outer Space*, 44, 48, in PEACEFUL AND NON-PEACEFUL USES OF PEACE, *supra* note 227.

[234] Morgan, *supra* note 207, at 304-305.

[235] Vlasic, *supra* note 233, at 45.

[236] *Id.*

the Law of Treaties,[237] therefore, the interpretation of the term "peaceful purposes" as meaning nonaggressive and not nonmilitary is the accurate interpretation.[238]

A useful comparison to the law of the sea can be made to support the view that "peaceful purposes" does not mean "nonmilitary." The law of the sea recognizes the right of armed vessels of a state to patrol the high seas to maintain, for example, the United Nations' commitment to maintaining international peace and security.[239] Also, as a matter of customary law and the Law of the Sea Convention, states may lawfully conduct military exercises on the high seas so long as they are carried out with due regard for the maintenance of other states' high seas freedoms.[240] As such, the law of the sea is a sufficiently comparable regime to the law of outer space to conclude that "peaceful purposes" in each regime has the same meaning.

As a post-script to this discussion, there have been attempts to classify particular military uses of outer space as peaceful or nonpeaceful and identify the uses that do violate the Outer Space Treaty. In this manner, the "nonaggressive" interpretation of "peaceful purposes" is acknowledged as the valid one but holds that not all military uses of outer space are peaceful. Certainly, the prohibited uses in Article IV of the Treaty are self-evident. A state could not, for example, station a nuclear missile launcher in outer space nor deploy other weapons of mass destruction there. Conversely, peaceful uses, which, because of states' tacit acceptance of them

---

[237] Vienna Convention on the Law of Treaties, 1155 U.N.T.S. 331, 8 I.L.M. 679 (1969); article 31 of the Vienna Convention provides that states' practice in the application of a treaty establishes their agreement regarding its interpretation.

[238] *Accord* Vlasic, *supra* note 233, at 44.

[239] Kunich, *supra* note 229, at 133.

[240] *Id.*

as not violating the Treaty, include communications, remote sensing, and navigation.[241]

Proposals to classify the following uses of spaces as nonpeaceful include: the use of force or the threat of the use of force in outer space or in the earth environment by a space object or being in outer space; the use of force or the threat of the use of force against a space object or a being in space by any method or means; and the use of space objects to assist in and aid military operations.[242] Other proposed delimitations focus on those uses that have a destabilizing effect on international peace and security.[243]

These efforts are probably doomed for being overly inclusive and exclusive. One can readily see that satellite uses that "aid in military operations" do not pose a threat to international security when used, for example, by a carrier battle group for inter-group communications during a predeployment exercise. As such, this definition is too inclusive.

Also, the proposed limitations tend to focus primarily on nuclear and other weapons of mass destruction and do not always consider tactical weapons that are not traditionally classified as weapons of mass destruction. More pertinently, they do not really account for information warfare techniques. For example, it would undoubtedly be nonpeaceful for a state to initiate an attack by launching conventional weapons through space to strike another state's electrical power system, but the

---

[241] Morgan, *supra* note 207, at 317.

[242] Chandrashekar, *supra* note 227, at 83.

[243] Vlasic, *supra* note 233, at 48-49.

proposed limitations do not provide for this scenario. This definition, then, is too exclusive.

A better limitation based on the purposes of the particular activity, that is, for a benign purpose or for aggressive reasons, has been suggested.[244] This is a more flexible and realistic approach to determining whether a particular activity in space is peaceful or not. On this basis, use of a satellite to facilitate an aggressive means of information warfare would make that use nonpeaceful and, thus, prohibited by the Outer Space Treaty.

A related question would be whether the Outer Space Treaty proscribes the use of outer space in self-defense against an unquestionably aggressive use of force in violation of article 2(4) of the Charter. Despite the clarity of Article 51, some writers hold that the Outer Space Treaty precludes the use of force in outer space even as a defensive measure.[245] Some view Article 51 as being neutralized by the *lex specialis* nature of the Outer Space Treaty.[246]

Conversely, assuming the "nonmilitary" view of the "peaceful purposes" clause is correct, self-defense should be seen as a special exception to this rule because the application of international law in outer space implies that States may exercise their right of self-defense against space activities of other States.[247]

---

[244] *E.g.*, Morgan, *supra* note 207, at 305-307.

[245] Chandrashekar, *supra* note 227, at 82; Morgan, *supra* note 207, at 308; Hurwitz, *supra* note 226 at 71.

[246] Hurwitz, *supra* note 226, at 72.

[247] *Id.*

The prevailing view, though, is that the Outer Space Treaty does not preclude the use of force in self-defense in outer space.[248] The well-established rule for the United States that "peaceful purposes" includes the right of self-defense was stated by Senator Al Gore, Sr., in a speech to the U.N. General Assembly in 1962:

> It is the view of the United States that outer space should be used only for peaceful—that is nonaggressive and beneficial—purposes. The question of military activities in space cannot be divorced from the question of military activities on earth. [. . .] [T]he test of any space activity must not be whether it is military or nonmilitary, but whether or not it is consistent with the UN Charter and other obligations of law. [249]

This right of self-defense in outer space is again analogous to the right of self-defense on the high seas. Although the Law of the Sea Convention provides for the use of the high seas for peaceful purposes, as a long-standing matter of customary law, a state has always retained the right to defend itself against the use of force on the high seas.[250]

The issues involving the right to anticipatory self-defense, what acts may be considered to violate article 2(4) and permitting the use of defensive force pursuant to article 51, and the principles of necessity, proportionality, and humanity, each discussed earlier, also apply in this context. In summary, if a state uses outer space in

---

[248] Hurwitz, *supra* note 226, at 73; Morgan, *supra* note 207, at 308.

[249] UN Doc A/C 1/PV. 1289 at 13 (1962), quoted in Kunich, *supra* note 229, at 133-134. Senator Gore's speech was equally influential in setting forth the U.S. policy position on the meaning of the "peaceful purposes" provision of the Outer Space Treaty.

[250] Hurwitz, *supra* note 226, at 73; Kunich, *supra* note 229, at 133.

an aggressive manner in violation of article 2(4) of the U.N. Charter, that state would also violate the requirement of the Outer Space Treaty to use outer space for peaceful purposes. The object state would be permitted to respond, even in outer space, pursuant to article 51 of the Charter. It is arguable whether a state could employ measures in outer space in anticipation of an aggressive attack, but, based on states' practice, anticipatory measures probably could be taken without violating the Charter or the Outer Space Treaty.

III. Conclusion

The foregoing article has shown that information warfare is a concept and method of conducting warfare that currently is in a nascent stage and difficult to circumscribe.[251] This article has reviewed how traditional concepts of the laws of armed conflict found in conventional and customary law may limit the ways information warfare is used a means of war and in self-defense. One senses that the use of information warfare by a state's military forces will qualify as a use of force, but the current problem is in determining when the threshold to qualify as a use of force is crossed. That is, it is difficult to say whether a particular use of information warfare is or is not "force."

---

[251] Indeed, as a postscript, some methods of information warfare might arguably be subject to Protocol II (the Landmine Protocol) of the Conventional Weapons Convention since a logic bomb, for example, could be construed as a "manually emplaced . . . device designed to . . . damage and which [is] actuated by remote control or automatically after a lapse of time." Article 2.3, Protocol II, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, UNGA Doc. A/CONF. 95/15 (27 Oct. 1980), 19 I.L.M. 1523 (1980).

Whether information warfare qualifies as "force" will determine the applicability of the traditional laws of armed conflict and its subset of humanitarian law. Unless "force" exists, those laws will not apply.

This is not to say a use of information warfare not constituting a use of force will not be limited by other principles of international law. The Declarations on Intervention and Friendly Relations will be very important instruments in limiting the extent to which a state may engage in information warfare.

Assuming the laws of armed conflict apply, it will be challenging to define the limits of necessity and proportionality in employing information warfare techniques. The experience of the Persian Gulf War has shown that traditionally military targets like electrical power systems and other information-based systems may possibly be evolving into impermissible targets because of the interconnection and interdependence of those systems with the civilian population.

Additionally, information warfare will test the limits of the concepts of neutrality and espionage. The application of principles of neutrality will depend in part on the ability of states to identify discrete portions of the GII that legitimately can be called sovereign territory. Without such designations, it will be difficult to locate neutral areas in the GII except for tangible objects like satellites and computer hardware.

Similarly, it will be difficult to find some state has engaged in espionage in the non-hardware portions of a state's NII without such designations. Since espionage is dependent on notions of territoriality, the existence of such "territory" in the NII will be a predicate applying this principle to information warfare. It is more

likely that states will not expand this concept and will instead limit its application to situations where its computer hardware and other physical components of national information systems are actually invaded or accessed.

The converse solution to these related issues, identifying international and, hence, non-sovereign areas in the GII, is unlikely to occur. The more probable solution will be to attempt to carve the GII into sovereign areas similar to the way national and international airspaces have developed in the law of aviation.

The law of outer space and international telecommunications may serve a role in limiting the use of information warfare. What constitutes permissible or nonpermissible uses of the GII could be facilitated by the understanding of "peaceful purposes" under the Outer Space Treaty. These laws will complement the proscriptions in the U.N. Charter regarding the use of force and threat of aggression. These laws, like the Charter, will not, however, prohibit the use of force in self-defense.

As for self-defense, information warfare promises to raise again the questions of whether a state must first receive an armed attack before responding, whether a state may engage in anticipatory self-defense, and whether particular responses are appropriately proportionate. As a sub-issue, the question whether the concept of reprisal is a valid principle of international law, or whether it is really dressed up as anticipatory self-defense, will be raised as well.

The outer limits of permissible information warfare, obviously, are not defined clearly. The development of those limits may in all likelihood follow the

course taken in the efforts to delimit outer space where the shape of the technology will help to define the contours of those limits.

In addition to states' efforts to define domestic crimes and, by implication, the limits of jurisdiction and sovereignty, it has been suggested that another way to deter information assault is to reach agreement among states as to what will actually constitute an assault on sovereignty.[252] This would stabilize relations in the information warfare arena and prevent those currently unavoidable scenarios where one state engages in tactics considered by another state to be an affront to its territorial integrity.[253]

The international organizations devoted to telecommunications should serve an important role in developing the limits of information warfare. In a best case scenario, these organizations will enable states to reach consensus on how best to peaceably use the GII for the common benefit. In the worst case scenario, the organizations should help to preserve the integrity and utility of the GII for those states not parties to an international conflict.

States should proceed with caution in developing new principles or norms solely in the context of the law of armed conflict since the methods of information warfare are still developing. Quickly rushing to create new norms risks developing a regime that is either too broad or too restrictive – leaving too many gaps to be filled or exceptions to be made. It is probably more prudent to apply the existing Charter framework of nonintervention, force, and self-defense to developing notions of

---

[252] Thomas, *supra* note 31 at 88-89.

[253] *Id.*

information warfare and to promote common understanding of acts that would be considered to fall into the range between "acceptable" coercion and impermissible force.

Nonetheless, consensus on the division between acts of force and those not considered to be force is essential. It is essential that the United Nations place this matter on its agenda and consider information warfare as a method of conducting international conflicts instead of considering only the criminal law enforcement aspects of it. The development of a common criminal code is one way to achieve an agreed way of applying international law to information warfare.

Included in such an agreement should be a willingness by states to prosecute persons found within a state's territory who commit computer-related offense that are consummated in another state. In so doing, states can begin to identify more precisely conduct that can be condemned by the international community as well as create an incentive to work together in a common way. An indirect result would be a better common understanding of acts that constitute "force" in violation of article 2(4) of the Charter. Once agreement on this concept of force is reached, the related issues of defensive measures, necessity, proportionality, and humanity should be made more amenable to resolution.

Much more data, though, about the uses, methods, and objectives of information warfare should be assembled before a comprehensive treaty can realistically be drafted. Creation of a committee in the U.N., similar to COPUOS, to receive information and serve as a central point for all of the participants in information warfare, is a good way to begin this process. While that committee was

initially formed in part to develop principles that would have prevented military involvement in outer space, it quickly saw the reality that the militaries of the Soviet Union and United States were the dominant actors in that new realm. Accordingly, it developed its principles on the beneficial use of outer space in a way that balanced competing military interests and legitimate interests of mankind. In like fashion, it may be possible, as more information is gathered about the potential uses and consequences of information warfare, to develop principles that promote peaceful uses of the GII while at the same time accounting for legitimate concerns for state security against foreign attacks. In so doing, order will be provided to the world's newest frontier.